ESSAI

SUR LA

THÉORIE DES NOMBRES;

PREMIERS ÉLÉMENTS,

PAR

T.-J. STIELTJES,

PROFESSEUR A LA FACULTÉ DES SCIENCES DE TOULOUSE.

SUR LA DIVISIBILITÉ DES NOMBRES.
DES CONGRUENCES. — ÉQUATIONS LINÉAIRES INDÉTERMINÉES.
SYSTÈMES DE CONGRUENCES LINÉAIRES.



PARIS,

GAUTHIER-VILLARS ET FILS, IMPRIMEURS-LIBRAIRES
DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,
Quai des Grands-Augustins, 55.

1895

ESSAI

SUR LA

THÉORIE DES NOMBRES

PREMIERS ÉLÉMENTS.

Extrait des *Annales de la Faculté des Sciences de Toulouse*, t. IV.

ESSAI

SUR LA

THÉORIE DES NOMBRES;

PREMIERS ÉLÉMENTS,

PAR

T.-J. STIELTJES,

PROFESSEUR A LA FACULTÉ DES SCIENCES DE TOULOUSE.

SUR LA DIVISIBILITÉ DES NOMBRES.
DES CONGRUENCES. — ÉQUATIONS LINÉAIRES INDÉTERMINÉES.
SYSTÈMES DE CONGRUENCES LINÉAIRES.



PARIS,

GAUTHIER-VILLARS ET FILS, IMPRIMEURS-LIBRAIRES
DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES,
Quai des Grands-Augustins, 55.

1895

SUR LA

THÉORIE DES NOMBRES.

CHAPITRE I.

SUR LA DIVISIBILITÉ DES NOMBRES.

1. L'idée de nombre a son origine dans la considération de plusieurs objets distincts.

C'est une notion qui s'attache à cette considération, où l'on fait abstraction de la nature des objets, et qui est, d'après notre conviction intime, indépendante de l'ordre dans lequel on envisage successivement les objets donnés.

Ce dernier point est essentiel et constitue, à proprement dire, le seul axiome de toute la science des nombres. Peut-être même est-il possible de ramener cet axiome à quelque chose de plus simple encore.

Si l'on se rappelle, en effet, que l'on peut passer d'une permutation à une autre par une série de transpositions opérées sur deux éléments voisins, il semble qu'au fond il suffit d'adopter l'axiome dans le cas de deux objets.

Mais, sans insister sur cette question, nous nous bornerons à observer que les relations exprimées par les équations

$$a+b=b+a, \qquad a+b+c=a+(b+c), \qquad \ldots$$
$$abc=bac=c(ab), \qquad \ldots$$
$$a(b+c)=ab+ac, \qquad \ldots$$

doivent être considérées comme des théorèmes qui découlent de l'axiome fondamental qui donne naissance à l'idée de nombre.

2. En comparant un nombre a avec les multiples o, b, $2b$, ... d'un second nombre b, deux cas peuvent se présenter. Ou bien a est égal à un multiple de b, alors a est divisible par b, b un diviseur de a, ou bien le nombre a tombe entre deux multiples consécutifs de b. Dans ce dernier cas, il existe un nombre m tel que $a = mb + c$, c étant positif, mais inférieur à b.

3. Étant donnés plusieurs nombres $a, b, c, \ldots, l$, on peut toujours trouver des nombres qui sont en même temps divisibles par a, par b, ..., par l. Parmi ces nombres qu'on appelle *communs multiples* de $a, b, c, \ldots, l$, il y en a un nécessairement qui est le plus petit et qui s'appelle le *plus petit commun multiple* des nombres $a, b, c, \ldots, l$.

Théorème I. — *Le plus petit commun multiple m des nombres $a, b, c, \ldots, l$ divise exactement tout autre commun multiple* M *de ces nombres.*

En effet, si M n'était pas un multiple de m, la division de M par m donnerait lieu à une relation

$$M = km + m',$$

où m' serait positif, mais inférieur à m. Or on reconnaît immédiatement que m' serait encore un commun multiple de $a, b, c, \ldots, l$, ce qui est absurde, puisqu'on suppose qu'il n'existe pas un tel commun multiple inférieur à m.

Il est clair qu'on peut énoncer ce théorème encore de cette manière :

Théorème I^a. — *Si un nombre* M *admet pour diviseurs les nombres $a, b, c, \ldots, l$, le plus petit commun multiple de $a, b, c, \ldots, l$ sera encore un diviseur de* M.

4. Le plus petit commun multiple des nombres

$$a > b > c > \ldots > l$$

est évidemment au moins égal à a, et il ne peut être égal à a que dans le cas où $b, c, \ldots, l$ sont des diviseurs de a.

5. Un nombre qui divise à la fois $a, b, c, \ldots, l$ s'appelle un *commun diviseur* de ces nombres. Parmi ces communs diviseurs, il y en a nécessairement un, plus grand que les autres, et qui s'appelle le *plus grand commun diviseur* de a, $b, c, \ldots, l$.

Théorème II. — *Le plus grand commun diviseur δ des nombres $a, b, c, \ldots, l$ est un multiple de tout autre commun diviseur δ' de ces nombres.*

Soient, en effet, δ, δ', δ'', ... les communs diviseurs des nombres donnés.

Puisque a est divisible par $\delta, \delta', \delta'', \ldots$, il est encore divisible par le plus petit commun multiple de $\delta, \delta', \delta'', \ldots$, et il en est de même pour $b, c, \ldots, l$. Par conséquent, le plus petit commun multiple de $\delta, \delta', \delta'', \ldots$ est encore un commun diviseur de $a, b, c, \ldots, l$. Ce plus petit commun multiple est donc nécessairement égal à δ, et $\delta', \delta'', \ldots$ sont les diviseurs de δ. L'ensemble des communs diviseurs de $a, b, c, \ldots, l$ est identique avec l'ensemble des diviseurs de δ.

6. Pour chercher le p. g. c. d. (p. p. c. m.) de $a, b, c, \ldots, l$, on peut diviser ces nombres en divers groupes, chercher le p. g. c. d. (p. p. c. m.) des nombres contenus dans ces groupes, ensuite le p. g. c. d. (p. p. c. m.) des nombres ainsi obtenus.

On pourra donc ramener le problème toujours au cas où il n'y a que deux nombres a et b, et, dans ce cas, l'algorithme d'Euclide conduit de la façon la plus simple à la connaissance du p. g. c. d. Par une suite de divisions, on obtient les relations

$$\begin{aligned}
a &= qb + r,\\
b &= q'r + r',\\
r &= q''r' + r'',\\
&\ldots\ldots\ldots\ldots\\
r^{(k-1)} &= q^{(k+1)} r^{(k)} + r^{(k+1)},\\
r^{(k)} &= q^{(k+2)} r^{(k+1)},
\end{aligned}$$

et $r^{(k+1)}$ est le p. g. c. d. de a et b.

Soit δ le p. g. c. d. de $a, b, c, \ldots, l$, alors les nombres $ma, mb, \ldots, ml$ sont tous divisibles par $m\delta$, leur p. g. c. d. est donc nécessairement divisible par $m\delta$, mais on reconnaît immédiatement que ce p. g. c. d. est exactement $m\delta$.

Pour abréger, nous emploierons quelquefois les symboles

$$(a, b, c, \ldots, l),$$
$$|a, b, c, \ldots, l|$$

pour désigner respectivement le p. g. c. d. et le p. p. c. m. de $a, b, \ldots, l$.

On a donc

$$(ma, mb, \ldots, ml) = m \times (a, b, \ldots, l)$$

et de même

$$|ma, mb, \ldots, ml| = m \times |a, b, \ldots, l|.$$

De là on peut conclure le lemme suivant qui est souvent utile.

Lemme. — *Soient d le p. g. c. d. (p. p. c. m.) des ν nombres*

$$a, \quad a', \quad a'', \quad \ldots.$$

e le p. g. c. d. (p. p. c. m.) des β *nombres*

$$b,\quad b',\quad b'',\quad \ldots$$

alors le p. g. c. d. (p. p. c. m.) des $\alpha\beta$ *produits*

$$ab,\quad ab',\quad ab'',\quad \ldots\qquad a'b,\quad a'b',\quad \ldots\qquad a''b,\quad a''b',\quad \ldots$$

est de.

En effet, les p. g. c. d. (p. p. c. m.) des divers groupes

$$\begin{array}{llll} ab, & ab', & ab'' & \ldots, \\ a'b, & a'b', & a'b'', & \ldots, \\ a''b, & a''b', & a''b'', & \ldots, \\ \ldots & \ldots & \ldots, & \ldots \end{array}$$

sont respectivement ae, $a'e$, $a''e$, ..., et le p. g. c. d. (p. p. c. m.) de ces derniers nombres est de.

7. La recherche du p. p. c. m. peut se ramener toujours à celle du p. g. c. d., et réciproquement.

Le p. p. c. m. de a, b, c est de la forme

$$\frac{abc}{d} = a \times \frac{bc}{d} = b \times \frac{ca}{d} = c \times \frac{ab}{d},$$

donc d doit être un commun diviseur de bc, ca, ab. Pour avoir le p. p. c. m., il faut évidemment prendre pour d le p. g. c. d. de bc, ca, ab.

Théorème III. — *Le p. p. c. m. (p. g. c. d.) de* $a, b, c, \ldots, l$ *est égal au produit* $abc\ldots l$ *divisé par le p. g. c. d. (p. p. c. m.) des produits*

$$bc\ldots l,\quad ac\ldots l,\quad \ldots,\quad abc\ldots k.$$

8. Dans le cas de deux nombres a et b, le produit du p. g. c. d. et du p. p. c. m. est ab. Cette relation n'a plus lieu dans le cas où l'on a n nombres. Cependant on peut rétablir l'analogie, et il faut, pour cela, considérer, non seulement le p. g. c. d. et le p. p. c. m., mais une suite de n nombres qui dérivent d'une façon particulière des nombres donnés.

Nous allons entrer dans quelques détails sur cette théorie, comprise dans des recherches plus générales de M. Smyth dont nous aurons à parler plus loin.

Considérons n nombres

(A) $$a,\quad b,\quad c,\quad \ldots,\quad l$$

Prenons deux nombres, par exemple a et b, de ce système et remplaçons-les par leur p. g. c. d. et leur p. p. c. m. On aura ainsi un second système (A_1)

$$a',\ b',\ c,\ \ldots,\ l.$$

En répétant la même opération sur (A_1) pour en déduire un système (A_2), puis un système (A_3), ..., on finira toujours par obtenir un système dans lequel deux nombres quelconques sont eux-mêmes leur p. g. c. d. et p. p. c. m., c'est-à-dire l'un de ces nombres divise l'autre. Si l'on ordonne les nombres de ce système définitif par ordre de grandeur croissante

$$e_1,\ e_2,\ e_3,\ \ldots,\ e_n,$$

e_k divise e_{k+1}, et nous dirons que ces nombres forment le système *réduit*, e_k est le $k^{\text{ième}}$ nombre réduit. En effet, on verra que ce système réduit est unique et indépendant de la manière dont on a dirigé les opérations.

9. Pour faciliter un peu le langage, nous dirons que deux nombres forment un couple réduit lorsque l'un de ces nombres divise l'autre. Il est clair que, si a et b sont un couple réduit, les groupes (A) et (A_1) sont identiques; on peut donc se dispenser de combiner les couples réduits. Si tous les couples de (A) étaient réduits, ce groupe serait déjà le système réduit.

Nous allons faire voir qu'en combinant deux nombres qui ne forment pas un couple réduit, on augmente toujours le nombre total des couples réduits.

Considérons, pour cela, les divers couples réduits de (A). On peut distinguer les quatre catégories suivantes :

1° Les couples réduits f, g qui ne renferment ni a, ni b. Il est bien clair que ces couples réduits se retrouvent dans (A_1).

2° Les couples réduits a, f qui renferment le nombre a et qui sont tels que b, f n'est pas un couple réduit. Dans ce cas, au moins un des couples a', f et b', f sera réduit, et ils peuvent l'être tous les deux. En effet, si f divise a, il est clair qu'il divise aussi b', et, si f est multiple de a, il sera aussi multiple de a'. [On suppose $a' = (a, b)$, $b' = [a, b]$.]

3° Les couples réduits b, f qui renferment le nombre b et qui sont tels que a, f n'est pas un couple réduit. Il est clair que ce que nous venons de dire pour le second cas s'applique encore ici.

4° Les couples réduits a, f qui sont tels que b, f est en même temps un couple réduit. Dans ce cas, on reconnaît facilement que les couples a', f et b', f sont aussi réduits tous les deux. Il suffit d'examiner successivement les trois hypothèses possibles : f divise a et b; f est multiple de a et de b; f divise l'un des nombres a, b et est multiple de l'autre.

Nous avons ainsi énuméré déjà dans le système (A_1) au moins autant de couples réduits que dans (A). Mais le système (A_1) renferme encore le couple réduit a', b', par conséquent le nombre des couples réduits du système (A_1) surpasse au moins d'une unité le nombre des couples réduits de (A).

Par un nombre fini d'opérations, on arrivera donc nécessairement à un groupe de n nombres dont tous les couples sont des couples réduits, et qui est ainsi le système réduit. Il reste à faire voir que ce système réduit est unique.

10. On constate d'abord qu'en remplaçant a et b par a' et b', on ne change ni le p. g. c. d., ni le p. p. c. m. des nombres du système.

Envisageons maintenant les divers produits k à k des nombres (A), pour voir quelles modifications résultent, pour ces produits, par le remplacement de a et b par a' et b'.

Les divers produits k à k se composent :

1° Des produits qui ne renferment ni a, ni b;
2° Des produits qui renferment a et b;
3° Des produits qui renferment un seul des nombres a et b.

Il est clair que ce sont les derniers produits seulement qui sont affectés par le remplacement de a et b par a' et b'. Ces produits sont, d'ailleurs, en nombre pair et peuvent être écrits ainsi

$$\begin{array}{lllll} aP, & aP', & aP'', & aP''', & \ldots, \\ bP, & bP', & bP'', & bP''', & \ldots, \end{array}$$

P, P', P'', ... étant les divers produits $k-1$ à $k-1$ des nombres $c, \ldots, l$.

En remplaçant maintenant a et b par a' et b', cela revient évidemment à remplacer chaque couple

$$(aP, bP), \quad (aP', bP'), \quad (aP'', bP''), \quad \ldots$$

par son p. g. c. d. et son p. p. c. m. Cette opération, nous l'avons déjà remarqué, n'influe ni sur le p. g. c. d., ni sur le p. p. c. m. des divers produits k à k.

Par conséquent, le p. g. c. d. D_k et le p. p. c. m. M_k des divers produits k à k des nombres (A) ne changent pas en passant aux nombres (A_1). D_k et M_k sont aussi le p. g. c. d. et le p. p. c. m. des produits k à k du système réduit

$$e_1, \quad e_2, \quad \ldots, \quad e_n,$$

c'est-à-dire

$$D_k = e_1 e_2 \ldots e_k, \qquad M_k = e_n e_{n-1} \ldots e_{n-k+1}.$$

De là on conclut les relations suivantes

$$e_1 = D_1, \quad e_2 = \frac{D_2}{D_1}, \quad \ldots, \quad e_k = \frac{D_k}{D_{k-1}}, \quad \ldots, \quad e_n = \frac{D_n}{D_{n-1}},$$

$$e_n = M_1, \quad e_{n-1} = \frac{M_2}{M_1}, \quad \ldots, \quad e_{n-k+1} = \frac{M_k}{M_{k-1}}, \quad \ldots, \quad e_1 = \frac{M_n}{M_{n-1}},$$

qui mettent en évidence ce fait que le système réduit est unique et donnent l'expression des nombres réduits en fonction de $a, b, c, \ldots, l$. Les relations

$$e_1 = D_1 = M_n : M_{n-1}, \qquad e_n = M_1 = D_n : D_{n-1}$$

reproduisent le théorème III. Puisque e_k divise e_{k+1}, on voit que D_k^2 divise $D_{k+1} D_{k-1}$, M_k^2 est multiple de $M_{k+1} M_{k-1}$; on pourrait le démontrer directement en s'appuyant sur le lemme du n° 6. On voit que D_k ne peut être égal à D_{k-1}, à moins qu'on n'ait $D_1 = D_2 = \ldots = D_k = 1$.

11. Lemme. — *a' et b' étant le p. g. c. d. et le p. p. c. m. de a et b, le p. g. c. d. et le p. p. c. m. de*

$$(m, a) \quad \text{et} \quad (m, b)$$

sont respectivement

$$(m, a') \quad \text{et} \quad (m, b').$$

De même, le p. g. c. d. et le p. p. c. m. de

$$|m, a| \quad \text{et} \quad |m, b|$$

sont respectivement

$$|m, a'| \quad \text{et} \quad |m, b'|.$$

Pour démontrer la première partie, on remarque d'abord que le p. g. c. d. de (m, a) et (m, b) est évidemment $(m, a, b) = (m, a')$. Cela étant, pour démontrer que (m, b') est le p. p. c. m. de (m, a) et (m, b), il suffira de faire voir que

$$(m, a) \times (m, b) = (m, a') \times (m, b').$$

Mais cela est évident; car, d'après le lemme du n° 6, on a

$$(m, a) \times (m, b) = (m^2, ma, mb, ab) = (m^2, ma', ab),$$
$$(m, a') \times (m, b') = (m^2, ma', mb', a'b') = (m^2, ma', a'b').$$

Pour la seconde partie, on remarque d'abord que le p. p. c. m. de $|m, a|$ et $|m, b|$ est évidemment $|m, a, b| = |m, b'|$; et ensuite il est clair que

$$|m, a| \times |m, b| = |m, a'| \times |m, b'|.$$

On conclut de ce lemme que les nombres réduits de

$$(m, a), \quad (m, b), \quad (m, c), \quad \ldots, \quad (m, l)$$

sont

$$(m, e_1), \quad (m, e_2), \quad (m, e_3), \quad \ldots, \quad (m, e_n).$$

De même, les nombres réduits de

$$|m, a|, \quad |m, b|, \quad |m, c|, \quad \ldots, \quad |m, l|$$

sont

$$|m, e_1|, \quad |m, e_2|, \quad |m, e_3|, \quad \ldots, \quad |m, e_n|.$$

12. Nous avons considéré, dans le n° 10, les divers produits k à k des nombres $a, b, c, \ldots, l$. Si, au lieu de cela, on avait considéré simplement les divers groupes k à k, non pour en former les produits, mais pour en prendre le p. g. c. d. ou le p. p. c. m., on serait arrivé aux résultats suivants :

e_1 est le p. g. c. d. de $|a|, |b|, |c|, \ldots, |l|$;
e_2 » $|a, b|, |a, c|, \ldots, |k, l|$;
e_3 » $|a, b, c|, |a, b, d|, \ldots$;
. . . . ;

puis aussi

e_n est le p. p. c. m. de $(a), (b), \ldots, (l)$;
e_{n-1} » $(a, b), (a, c), \ldots, (k, l)$;
e_{n-2} » $(a, b, c), (a, b, d), \ldots$;
. . . .

Cette recherche n'offre aucune difficulté en s'appuyant sur le lemme du n° 11.

13. On dit que deux nombres sont premiers entre eux (ou bien a est premier avec b) lorsque leur p. g. c. d. est égal à l'unité; leur p. p. c. m. est alors égal à leur produit.

Lemme. — *On a*

$$(a, bc) = (a, c \times (a, b)).$$

En effet, il est clair que

$$(a, bc) = (a, bc, ac),$$

or

$$(bc, ac) = c \times (a, b).$$

Théorème IV. — *Lorsque a et b sont premiers entre eux, tout commun diviseur de a et bc est aussi commun diviseur de a et c.*

Il suffit évidemment de montrer que

$$(a, bc) = (a, c).$$

mais cela est évident d'après le lemme précédent, puisque $(a, b) = 1$ par hypothèse.

On déduit de ce théorème les conséquences suivantes : 1° Si c est aussi premier avec a, bc est premier avec a. Il est facile de généraliser ce résultat ainsi. Les nombres

$$a,\quad a',\quad a'',\quad \ldots,$$
$$b,\quad b',\quad b'',\quad \ldots,$$

étant tels que chaque nombre $a, a', \ldots$ est premier avec tous les nombres $b, b', \ldots$, le produit $aa'a''\ldots$ est premier avec $bb'b''\ldots$, a^m est premier avec b^n. 2° Lorsque bc est divisible par a (a et b étant premiers entre eux), c est divisible par a.

14. On dit que plusieurs nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque deux quelconques d'entre eux le sont. On peut remplacer cette définition par la suivante qui lui est équivalente. Plusieurs nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque a est premier avec $bc\ldots l$, b avec $cd\ldots l$, ..., enfin k avec l.

Le p. p. c. m. des nombres $a, b, c, \ldots, l$, qui sont premiers entre eux, est égal à leur produit, et cette propriété est caractéristique. En effet, ayant

$$|a, b, c, \ldots, l| = abc\ldots l,$$

il est impossible que deux de ces nombres aient un diviseur commun > 1. Car, si δ divise a et b,

$$\frac{ab}{\delta} \times cd\ldots l$$

est un commun multiple de $a, b, c, \ldots, l$.

Un nombre admettant les diviseurs $a, b, c, \ldots, l$ premiers entre eux, est divisible par leur produit $abc\ldots l$.

On peut dire encore : les nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque le $(n-1)^{\text{ième}}$ nombre réduit $e_{n-1} = 1$. En effet, e_{n-1} est le p. p. c. m. des nombres

$$(a, b),\quad (a, c),\quad (b, c),\quad \ldots,\quad (k, l).$$

On a alors aussi

$$e_1 = e_2 = \ldots = e_{n-2} = e_{n-1} = 1,$$
$$e_n = abc\ldots l.$$

Pour que plusieurs nombres $a, b, c, \ldots, l$ soient premiers entre eux, il ne suffit pas que leur p. g. c. d. soit égal à l'unité, il faut que le p. g. c. d. D_{n-1} des produits

$$bc\ldots l,\quad ac\ldots l,\quad \ldots,\quad abc\ldots k$$

soit égal à l'unité. (*Voir* le théorème III et la fin du n° 10.)

Lemme. — *Le p. g. c. d. des nombres m, a, b étant l'unité, on a*

$$(m, ab) = (m, a) \times (m, b).$$

En effet, d'après le lemme du n° 6,

$$(m, a) \times (m, b) = (m^2, ma, mb, ab).$$

Or

$$(m^2, ma, mb) = m \times (m, a, b) = m$$

d'après l'hypothèse.

Plus particulièrement, on aura

$$(m, ab) = (m, a) \times (m, b)$$

lorsque a et b sont premiers entre eux. Ce résultat peut se généraliser immédiatement ainsi.

Théorème V. — *Les nombres a, b, c, ..., l étant premiers entre eux, on a*

$$(m, abc\ldots l) = (m, a) \times (m, b) \times (m, c) \times \ldots \times (m, l).$$

Remarque. — Ce résultat est compris aussi comme cas particulier dans les propositions obtenues dans le n° 11. En effet, le $n^{\text{ième}}$ nombre réduit de

$$(m, a), \quad (m, b), \quad (m, c), \quad \ldots, \quad (m, l),$$

c'est-à-dire leur p. p. c. m. est égal à

$$(m, e_n) = (m, | a, b, c, \ldots, l |).$$

En supposant $a, b, c, \ldots, l$ premiers entre eux, on retrouve le théorème ci-dessus. On peut en tirer la conséquence que voici. Les nombres $a, b, c, \ldots, l$ étant premiers entre eux, un diviseur δ de leur produit peut être toujours mis d'une seule façon sous la forme

$$\delta = a'b'c'\ldots l',$$

où a' divise a, b' divise b, ..., l' divise l. En effet, si cette décomposition en facteurs est possible, a' doit diviser a et δ, et par conséquent (a, δ).

Mais, d'après le théorème V, on a

$$\delta = (a, \delta) \times (b, \delta) \times \ldots \times (l, \delta);$$

d'où il est clair que la décomposition est possible, et d'une seule manière.

D'autre part, on obtient toujours un diviseur de $abc\ldots l$, en multipliant un diviseur quelconque a' de a par un diviseur b' de b, etc.

On peut donc conclure :

Théorème VI. — *Les nombres a, b, c, ..., l étant premiers entre eux, on obtient tous les diviseurs de leur produit $abc \dots l$, et chaque diviseur une seule fois, en multipliant chaque diviseur de a par chaque diviseur de b, ..., par chaque diviseur de l.*

Corollaire. — En désignant par $f(m)$ le nombre des diviseurs de m (ou la somme de ces diviseurs, ou la somme de leurs $k^{\text{ièmes}}$ puissances), on a

$$f(abc \dots l) = f(a) \times f(b) \times f(c) \times \dots \times f(l)$$

lorsque a, b, c, ..., l sont premiers entre eux.

15. Tout nombre a (excepté l'unité) a au moins les deux diviseurs a et 1. Tout nombre qui n'admet pas d'autres diviseurs s'appelle nombre *premier*. Nous ne compterons pas l'unité parmi les nombres premiers : les plus petits nombres premiers sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \dots$$

Tout nombre qui n'est pas premier est dit *composé*. Un nombre composé a est toujours égal à un produit bc dont les facteurs sont > 1 tous les deux.

Soient p un nombre premier, a un nombre quelconque ; si p ne divise pas a, a et p seront premiers entre eux.

Lorsqu'un nombre premier p divise le produit $abc \dots l$, p doit diviser au moins un des facteurs a, b, c, ..., l ; car, dans le cas contraire, p serait premier avec a, avec b, ..., avec l, par conséquent premier avec $abc \dots l$ et ne pourrait diviser ce produit.

Théorème VII. — *Tout nombre composé admet un diviseur premier.*

En effet, il est clair que le plus petit diviseur, surpassant l'unité, d'un nombre composé, est nécessairement un nombre premier.

Théorème VIII. — *Tout nombre composé est égal à un produit de facteurs premiers ou, comme on dit, il est décomposable en facteurs premiers. Cette décomposition ne peut se faire que d'une seule manière.*

En effet, mettons le nombre composé a sous la forme d'un produit

$$bc \dots l$$

de facteurs > 1, de toutes les manières possibles. Le nombre de ces facteurs sera toujours inférieur à n, en supposant $2^n > a$. Parmi ces produits égaux à a, il y en aura donc un, au moins, dans lequel le nombre des facteurs est le plus grand.

Soit

$$p_1 p_2 \ldots p_k$$

un tel produit, il est clair que tous les facteurs sont des nombres premiers; car, si par exemple p_1 était composé, on pourrait obtenir un produit égal à a et renfermant $k+1$ facteurs.

Remarque. — Il est clair qu'on obtient toujours par un nombre fini d'essais les divers produits égaux à a que nous considérons. Il suffit d'écrire les nombres

$$2, \quad 3, \quad 4, \quad \ldots, \quad a,$$

de prendre leurs divers produits un à un, deux à deux, ..., $n-1$ à $n-1$ (avec répétitions) et de ne conserver que ceux de ces produits qui sont égaux à a.

La première partie du théorème se trouve ainsi démontrée; quant à la seconde partie, supposons deux décompositions en facteurs premiers

$$a = p_1 p_2 p_3 \ldots = q_1 q_2 q_3 \ldots.$$

Il est clair que q_1 doit diviser le produit $p_1 p_2 p_3 \ldots$, et, par conséquent, un des nombres $p_1, p_2, p_3, \ldots$: donc q_1 est égal à un de ces nombres, par conséquent $p_1 = q_1$.

On en conclut

$$p_2 p_3 \ldots = q_2 q_3 \ldots;$$

d'où

$$p_2 = q_2, \quad \ldots.$$

Le théorème étant ainsi complètement démontré, on voit qu'on peut mettre un nombre quelconque, et cela d'une seule manière, sous la forme

$$p^\alpha q^\beta r^\gamma \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers distincts, $\alpha, \beta, \gamma, \ldots$ des nombres quelconques.

On peut déduire ce théorème aussi du théorème VII.

16. Pour que deux nombres soient divisibles l'un par l'autre, il faut et il suffit qu'en ayant décomposé les deux nombres en facteurs premiers le diviseur n'ait pas d'autres facteurs premiers que le dividende, et que ces facteurs ne figurent pas dans le diviseur avec de plus grands exposants que dans le dividende. Cela est évident d'après ce qui précède.

A l'aide de ce résultat, on peut reconnaître immédiatement la vérité de tous les théorèmes que nous avons obtenus sur le p. p. c. m., le p. g. c. d., etc., en supposant tous les nombres décomposés en facteurs premiers. Nous n'insisterons pas sur ce sujet, cependant on doit remarquer que ce n'est là, à proprement

parler, qu'une espèce de vérification ; cela devient sensible surtout lorsqu'il s'agit de propositions plus compliquées, comme celles du n° 11 sur les nombres réduits. Mais nous devons expliquer encore comment on obtient immédiatement les nombres réduits de $a, b, c, \ldots, l$, lorsqu'on a décomposé ces nombres en facteurs premiers.

Supposons donc

$$
\begin{aligned}
a &= p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},\\
b &= p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k},\\
c &= p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
l &= p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}.
\end{aligned}
$$

Pour plus de symétrie, nous avons introduit partout les mêmes nombres premiers $p_1, p_2, \ldots, p_k$, ce qui peut se faire en admettant pour les exposants aussi la valeur o.

Considérons les exposants de p_i

$$\alpha_i, \quad \beta_i, \quad \gamma_i, \quad \ldots, \quad \lambda_i.$$

Supposons qu'en les écrivant par ordre de grandeur croissante on ait

$$a_i \leqq b_i \leqq c_i \leqq \ldots \leqq l_i.$$

Alors on aura

$$
\begin{aligned}
e_1 &= p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k},\\
e_2 &= p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k},\\
e_3 &= p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
e_n &= p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}.
\end{aligned}
$$

C'est ce qu'on vérifie directement en remarquant, par exemple, que

$$e_1 e_2 \ldots e_k = \mathrm{D}_k$$

est bien, avec ces valeurs de $e_1, e_2, \ldots, e_n$, le p. g. c. d. des produits k à k des nombres $a, b, c, \ldots, l$. On vérifie encore sans peine les expressions des e_k que nous avons obtenues dans le n° **12**.

Les diviseurs de p^α sont

$$1, \quad p, \quad p^2, \quad \ldots, \quad p^\alpha,$$

leur nombre est $\alpha + 1$, leur somme

$$\frac{p^{\alpha+1} - 1}{p - 1}.$$

Un nombre quelconque

$$p^\alpha q^\beta r^\gamma \ldots$$

admet donc

$$(\alpha+1)\times(\beta+1)\times(\gamma+1)\ldots$$

diviseurs, et leur somme est

$$\frac{p^{\alpha+1}-1}{p-1}\times\frac{q^{\beta+1}-1}{q-1}\times\frac{r^{\gamma+1}-1}{r-1}\times\ldots.$$

17. Décomposer un nombre donné en facteurs premiers, c'est un problème dont la solution exige un grand nombre de tâtonnements. On a imaginé de nombreux artifices pour abréger le travail; mais, quoi qu'on fasse, cette décomposition est, en réalité, impraticable pour un nombre un peu grand. Aussi serait-il, par exemple, à peu près impossible d'obtenir de cette façon le p. g. c. d. de deux nombres de douze à quinze chiffres; l'algorithme d'Euclide conduit sans trop de peine au but.

On voit par là que ce n'est pas seulement en se plaçant au point de vue théorique qu'on peut exiger de ne pas faire intervenir la décomposition en nombres premiers dans des questions où ces nombres premiers ne figurent pas expressément.

Il y a une infinité de nombres premiers. En effet, p étant un nombre premier, on peut toujours trouver un nombre premier plus grand que p. Soit, pour le montrer,

$$P = 2\times 3\times\ldots\times p$$

le produit de tous les nombres premiers qui ne surpassent pas p. Mettons le nombre P d'une façon quelconque sous la forme d'un produit de deux facteurs

$$P = AB,$$

alors il est clair que le nombre $N = A + B$ n'est divisible ni par 2, ni par 3, ..., ni par p. En décomposant donc N en facteurs premiers, on trouvera nécessairement des nombres premiers qui surpassent p.

Remarquons avec M. Cayley que, si l'on prend $A = P$, $B = 1$, les nombres $N+1$, $N+2$, ..., $N+p-1$ sont tous composés; d'où l'on voit que la différence de deux nombres premiers consécutifs peut surpasser un nombre donné.

18. Voici une proposition dont on a besoin quelquefois. Il est toujours possible de mettre le p. p. c. m. des nombres a, b, c, ..., l sous la forme d'un produit

$$a'b'c'\ldots l',$$

dont les facteurs sont premiers entre eux et divisent respectivement a, b, c, ... l. Adoptons les notations du n° 16, le p. p. c. m. est

$$p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}.$$

Écrivons les nombres a, b, c, ... l l'un au-dessous de l'autre. Écrivons ensuite le facteur $p_1^{l_1}$ à côté d'un des nombres a, b, c, ..., l qu'il divise (un au moins de ces nombres est divisible par $p_1^{l_1}$). Faisons de même pour $p_2^{l_2} \ldots p_k^{l_k}$. Alors on prendra pour a' le produit des nombres qu'on aura écrits à côté de a ($a' = 1$ lorsque aucun nombre ne se trouverait à côté de a), de même pour b', c', ..., l'.

Il est clair qu'on obtiendra toujours au moins une solution ; elle est unique dans le cas où, parmi les nombres a, b, ..., l, il n'y en a qu'un seul divisible, soit par $p_1^{l_1}$, soit par $p_2^{l_2}$, etc. Dans le cas contraire, le problème admet toujours plusieurs solutions.

19. On peut toujours obtenir une solution, sans décomposer les nombres a, b, c, ..., l en facteurs premiers et uniquement à l'aide de l'algorithme d'Euclide.

Mais, pour abréger, nous nous bornerons au cas de deux nombres a et b, d'où il est facile, du reste, de remonter au cas général. Soit $(a, b) = d$, et calculons

$$\left(\frac{a}{d}, d\right) = a', \qquad \left(\frac{b}{d}, d\right) = b';$$

a' et b' seront premiers entre eux, puisque $\frac{a}{d}$ et $\frac{b}{d}$ le sont ; d sera donc divisible par leur produit, soit

$$d = a'b'd'$$

et puis

$$\left(\frac{a}{d}, d'\right) = a'', \qquad \left(\frac{b}{d}, d'\right) = b'',$$

$$d' = a''b''d'',$$

$$\left(\frac{a}{d}, d''\right) = a''', \qquad \left(\frac{b}{d}, d''\right) = b'''.$$

$$d'' = a'''b'''d''',$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

En continuant ainsi, on finira toujours par arriver à un couple

$$a^{(k+1)} = 1, \qquad b^{(k+1)} = 1,$$

car

$$d = a'b'd' = a'a''b'b''d'' = a'a''a'''b'b''b'''d''' = \ldots$$

On aura alors

$$d = (a'a'' \ldots a^{(k)}) \times (b'b'' \ldots b^{(k)}) \times d^{(k)}$$

et, pour le p. p. c. m.,

$$m = \frac{ab}{d},$$

$$m = \left(\frac{a}{d} \times a'a''\ldots a^{(k)}\right) \times \left(\frac{b}{d} \times b'b''\ldots b^{(k)}\right) \times d^{(k)}.$$

Les nombres $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux, et, $a', a'', \ldots, a^{(k)}$ étant des diviseurs de $\frac{a}{d}$, $b', b'', \ldots, b^{(k)}$ des diviseurs de $\frac{b}{d}$, il est clair que les deux facteurs

$$\frac{a}{d} \times a'a''\ldots a^{(k)} \quad \text{et} \quad \frac{b}{d} \times b'b''\ldots b^{(k)}$$

sont premiers entre eux. Ensuite $d^{(k)}$ est premier avec chacun de ces facteurs, car

$$\left(\frac{a}{d}, d^{(k)}\right) = a^{(k+1)} = 1, \qquad \left(\frac{b}{d}, d^{(k)}\right) = b^{(k+1)} = 1.$$

En prenant donc

$$\text{A} = \frac{a}{d} \times a'a''\ldots a^{(k)},$$

$$\text{B} = \frac{b}{d} \times b'b''\ldots b^{(k)} \times d^{(k)},$$

on aura $m = \text{AB}$, A et B seront premiers entre eux, puis A divise a et B divise b. Plus généralement, si l'on a $d^{(k)} = pq$, p et q étant premiers entre eux, on pourra prendre

$$\text{A} = \frac{a}{d} \times a'a''\ldots a^{(k)} \times p,$$

$$\text{B} = \frac{b}{d} \times b'b''\ldots b^{(k)} \times q.$$

Si l'on suppose a et b décomposés en facteurs premiers, on verra facilement que

$$\frac{a}{d} \times a'a''\ldots a^{(k)}$$

est le produit des puissances de nombres premiers qui figurent dans la décomposition de a avec des exposants plus grands que dans la décomposition de b, tandis que $d^{(k)}$ est le produit des puissances de nombres premiers qui figurent avec le même exposant dans les décompositions de a et de b. Lorsqu'on a $d^{(k)} > 1$, on obtient toujours deux solutions au moins, en prenant soit $p = 1$, $q = d^{(k)}$, soit $p = d^{(k)}$, $q = 1$. Mais, dans ce cas, il peut arriver que le problème admet encore d'autres solutions, et cela a lieu lorsque $d^{(k)}$ est divisible par plus d'un nombre premier.

Mais, pour obtenir ces solutions, il faut absolument recourir à la décomposition de $d^{(h}$ en facteurs premiers : l'algorithme d'Euclide seul ne peut pas les faire connaître.

20. En jetant maintenant un coup d'œil sur le chemin que nous avons parcouru, on reconnaîtra que la théorie de la divisibilité des nombres repose sur ce fait, qu'étant donnés deux nombres a et b, on peut toujours déterminer un nombre m, tel que

$$a = mb + c,$$

où

$$0 \leqq c < b.$$

Si l'on considère les nombres complexes $a + bi(i = \sqrt{-1})$, on peut établir une relation analogue, et de là découle, pour ces nombres, une théorie de la divisibilité parfaitement analogue à celle des nombres ordinaires. Nous aurons à revenir plus tard sur cette question et d'autres de la même nature.

Les propositions les plus essentielles sur la divisibilité des nombres se trouvent déjà dans les *Éléments d'Euclide ;* notamment on y trouve : l'algorithme pour la recherche du plus grand commun diviseur, la proposition qu'un produit ne peut être divisible par un nombre premier, à moins qu'un des facteurs ne le soit, la proposition qu'il y a un nombre infini de nombres premiers.

CHAPITRE II.

DES CONGRUENCES.

1. Si la différence des deux nombres a et b est divisible par un nombre M, a et b sont dits *congrus* par rapport à M ; le diviseur M est appelé le *module ;* a et b sont *résidus l'un de l'autre* suivant le module M. Pour exprimer cette relation, on écrit, d'après la notation de Gauss,

$$a \equiv b \pmod{M};$$

cette formule est une *congruence*. Il y a avantage, dans cette théorie, à admettre, pour a et b, non seulement les valeurs entières positives, mais aussi les valeurs entières négatives.

Si r est le reste de la division de a par M, on a

$$a \equiv r \pmod{M};$$

le reste r est ordinairement un des nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1,$$

mais on pourrait le prendre aussi entre $-\frac{M}{2}$ et $+\frac{M}{2}$; d'où il suit que tout nombre a un résidu qui ne surpasse pas en valeur absolue la moitié du module. C'est là le *résidu minimum*.

2. Nous allons indiquer ici les propriétés les plus élémentaires des congruences, il sera à peine nécessaire d'insister sur les démonstrations. Si l'on n'indique pas le module, il sera sous-entendu que ce module est toujours M.

Si l'on a

$$a \equiv b, \qquad a' \equiv b', \qquad a'' \equiv b'', \qquad \ldots,$$

on aura ainsi

$$a + a' + a'' + \ldots \equiv b + b' + b'' + \ldots.$$

$$ma \equiv mb.$$

De même, on aura

$$aa' \equiv ba' \equiv bb'$$

et plus généralement

$$aa'a'' \ldots \equiv bb'b'' \ldots,$$

$$a^m \equiv b^m.$$

Ainsi

$$f(x, y, z, \ldots) = \sum A_{m,n,p,\ldots} x^m y^n x^p \ldots$$

étant un polynôme à coefficients entiers, on aura

$$f(a, a', a'', \ldots) \equiv f(b, b', b'', \ldots).$$

3. Supposons qu'on ait

$$ma \equiv mb \qquad (\bmod M),$$

ce qui signifie que $m(a-b)$ est divisible par M; soit

$$(m, M) = d,$$

$\frac{m}{d}(a-b)$ sera divisible par $\frac{M}{d}$, et, puisque $\frac{m}{d}$ et $\frac{M}{d}$ sont premiers entre eux, $a-b$ sera divisible par $\frac{M}{d}$: donc

$$a \equiv b \qquad \left(\bmod \frac{M}{d}\right).$$

On peut donc diviser les deux membres d'une congruence par un nombre m, à condition de diviser en même temps le module par le p. g. c. d. de m et M. On aura à appliquer cette proposition le plus souvent dans les cas particuliers suivants : 1° m est premier avec M, alors $d = 1$; 2° m divise M, alors $d = m$.

Supposons encore qu'on ait

$$aa' \equiv bb' \qquad (\bmod M),$$
$$a \equiv b \qquad (\bmod M).$$

En multipliant la seconde congruence par a', il vient, en faisant attention à la première,

$$ba' \equiv bb' \qquad (\bmod M),$$

donc

$$a' \equiv b' \qquad \left(\bmod \frac{M}{d}\right),$$

où $d = (b, M) = (a, M)$, car il est clair que des nombres congrus ont même p. g. c. d. avec le module.

Si deux nombres sont congrus suivant le module M, ils seront congrus encore en prenant pour module un diviseur de M. Si deux nombres sont congrus suivant plusieurs modules A, B, C, ..., L, ils seront congrus encore en prenant pour module le p. p. c. m. de ces nombres

$$M = \{A, B, C, \ldots, L\}.$$

Le cas particulier le plus intéressant est celui où les modules A, B, C, ..., L sont premiers entre eux, alors $M = ABC...L$.

4. On peut distribuer l'ensemble des nombres entiers en M *classes*, en considérant deux nombres comme appartenant à la même classe ou non, selon qu'ils sont congrus ou non suivant le module M. En prenant dans chaque classe un nombre, on obtient un groupe de M nombres, qu'on appelle un *système complet de résidus*. Un tel système jouit évidemment de la propriété qu'un nombre quelconque est congru à un et à un seul de ses nombres. Un nombre quelconque a pris dans une classe peut être considéré comme représentant la classe entière qui se compose des nombres $a + Mx$, $x = 0, \pm 1, \pm 2, \pm 3, \ldots$. On désigne ainsi souvent la classe par un quelconque des nombres qu'il renferme, et l'on peut ainsi remplacer un nombre par un nombre congru.

Tous les nombres d'une classe ont le même p. g. c. d. avec le module M, et ce p. g. c. d. peut être un diviseur quelconque d de M.

On peut, d'après cela, distribuer les classes en familles, en considérant diverses classes comme appartenant à une même famille, si elles ont le même p. g. c. d. avec le module M.

Combien de classes y a-t-il qui sont premières avec M? Il est clair qu'il y en a autant qu'on trouve parmi les nombres

$$(A) \qquad 1, \quad 2, \quad 3, \quad \ldots, \quad M$$

des nombres qui sont premiers avec M. Nous désignerons ce nombre par $\varphi(M)$, en sorte que

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \ldots.$$

Le nombre des classes qui ont avec M le p. g. c. d. d est évidemment le même que celui des nombres du groupe (A) qui ont d pour p. g. c. d. avec M. Il faudra donc les chercher parmi les nombres

$$d, \quad 2d, \quad 3d, \quad \ldots, \quad kd, \quad \ldots, \quad \frac{M}{d}d.$$

Or, pour que $(kd, M) = d$, il faut et il suffit que k soit premier avec $\frac{M}{d}\cdot$ Le nombre cherché indique donc combien, parmi les nombres

$$1, \quad 2, \quad 3, \quad \ldots, \quad \frac{M}{d},$$

il y en a qui sont premiers avec $\frac{M}{d}$, c'est-à-dire ce nombre est $\varphi\left(\frac{M}{d}\right)\cdot$

Il y a ainsi $\varphi\left(\frac{M}{d}\right)$ classes qui ont d pour p. g. c. d. avec M, le nombre total des classes étant M, on a

$$\sum \varphi\left(\frac{M}{d}\right) = M,$$

d parcourant tous les diviseurs de M. Il est clair qu'on peut écrire cette relation plus simplement ainsi

$$\sum \varphi(d) = M.$$

Il est facile de déduire de là la valeur de $\varphi(M)$.

5. Supposons plus généralement que deux fonctions numériques f et F soient liées par la relation

(1) $$F(M) = \sum f(d),$$

d parcourant tous les diviseurs de M. Nous allons exprimer réciproquement la fonction f au moyen de F.

Soit

$$M = p^\alpha q^\beta r^\gamma \ldots u^\lambda$$

la décomposition de M en facteurs premiers. On obtient l'ensemble des diviseurs d de M en développant le produit

$$M\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right),$$

et nous pouvons écrire d'une manière symbolique

$$F(M) = f\left| M\left(1 + \frac{1}{p} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

On doit développer le produit du second membre et remplacer ensuite chaque terme d par $f(d)$. En remplaçant M par $M:p$ (donc α par $\alpha - 1$), on aura

$$F\left(\frac{M}{p}\right) = f\left| M\left(\frac{1}{p} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

En retranchant, il vient, si l'on fait usage dans le premier membre de la même notation symbolique

$$F\left| M\left(1 - \frac{1}{p}\right)\right| = f\left| M\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\left(1 + \frac{1}{r} + \ldots + \frac{1}{r^\gamma}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

En remplaçant M par $\frac{M}{q}$ et retranchant, il vient ensuite

$$F\left|M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\right| = f\left|M\left(1+\frac{1}{r}+\ldots+\frac{1}{r^\gamma}\right)\ldots\left(1+\frac{1}{u}+\ldots+\frac{1}{u^\lambda}\right)\right|.$$

En continuant ainsi, on obtient finalement

$$(2)\qquad F\left|M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{u}\right)\right| = f(M);$$

c'est l'expression cherchée; on peut l'écrire plus explicitement

$$(2')\qquad f(M) = F(M) - \sum F\left(\frac{M}{p}\right) + \sum F\left(\frac{M}{pq}\right) - \sum F\left(\frac{M}{pqr}\right) + \ldots$$

On rencontre souvent des fonctions numériques qui jouissent de la propriété

$$(3)\qquad f(ab) = f(a)\times f(b)$$

lorsque a et b sont premiers entre eux (*voir* Chap. I, n° 14). Il est clair qu'une telle fonction est parfaitement déterminée lorsqu'on connaît sa valeur pour les puissances des nombres premiers, mais ces valeurs-là peuvent être prises arbitrairement.

On voit facilement que, si la fonction f qui figure dans la relation (1) jouit de cette propriété (3), on aura aussi, a et b étant premiers entre eux,

$$(4)\qquad F(ab) = F(a)\times F(b),$$

et l'on reconnaît maintenant par les formules (2) ou (2') que, réciproquement, si deux fonctions f et F sont liées par la relation (1), et si la fonction F satisfait à la relation (4), la fonction f satisfera à la relation analogue (3).

Le théorème, souvent utile, de ce numéro est dû à M. Dedekind (*Journal de Crelle*, t. 54, p. 21). On l'établit ordinairement par une simple vérification. En exprimant au second membre de (2') partout la fonction F par la fonction f, on constate qu'il ne reste que le terme $f(M)$: tous les autres termes se détruisent.

6. En revenant au cas particulier de la fonction $\varphi(M)$, $F(M) = M$, on trouve

$$\varphi(M) = M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{u}\right),$$
$$\varphi(M) = p^{\alpha-1}q^{\beta-1}\ldots u^{\lambda-1}(p-1)(q-1)\ldots(u-1).$$

Ayant $\varphi(ab) = \varphi(a)\varphi(b)$ lorsque a et b sont premiers entre eux, on peut remar-

quer que, a étant impair, on a, à cause de $\varphi(2) = 1$,

$$\varphi(2a) = \varphi(a).$$

A l'exception de $\varphi(1) = \varphi(2) = 1$, $\varphi(a)$ est toujours pair.

7. Dans la théorie des nombres, on se propose, sur les congruences, des problèmes analogues à ceux qu'on traite en Algèbre sur les équations.

Ainsi on pose la question de trouver les nombres x qui satisfont à une congruence, telle que

$$f(x) \equiv 0 \pmod{M},$$

où le premier membre est un polynôme à coefficients entiers en x.

Si l'on satisfait à cette congruence en faisant $x = x_0$, x_0 est une *racine* de la congruence. Il est clair que tout nombre congru à x_0 suivant le module M satisfera alors aussi à la congruence, mais on a l'habitude de ne pas considérer comme différentes ces solutions. Aussi, si l'on dit qu'une congruence admet k racines, cela veut dire k racines *incongrues*, ou encore, ce qui revient au même, l'ensemble des nombres qui satisfont à la congruence se répartit en k classes. Il est clair, d'après cela, qu'on obtient toutes les racines d'une congruence, en essayant successivement tous les nombres d'un système complet de résidus, par exemple les nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1,$$

mais ce moyen devient impraticable dès que M est un peu grand.

Si tous les coefficients du polynôme $f(x)$ sont divisibles par M, la congruence est *identique*, un nombre quelconque y satisfait. La congruence est impossible évidemment lorsque tous les coefficients de $f(x)$ sont divisibles par M, à l'exception du terme indépendant de x.

Il est clair, du reste, qu'il est permis de remplacer un coefficient quelconque de $f(x)$ par un nombre congru suivant le module M.

8. Considérons la congruence du premier degré

$$ax + b \equiv 0 \pmod{M}.$$

Supposons d'abord a premier avec M. Pour voir si la congruence admet des racines, mettons pour x successivement les valeurs

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1$$

ou, si l'on veut, M valeurs quelconques formant un système complet de résidus. Il est clair que les valeurs correspondantes de $ax + b$ sont incongrues, car la re-

lation

$$ax+b \equiv ay+b$$

exige qu'on ait $ax \equiv ay$ ou encore $x \equiv y$, puisque a est premier avec M.

Les valeurs de $ax+b$ forment donc également un système complet de résidus, et, parmi ces valeurs, il y en a donc *une* qui est congrue avec o. La congruence proposée admet donc *une* racine.

Supposons maintenant $(a, \mathrm{M}) = d$. Dans ce cas, il est clair que b doit être divisible par d; dans le cas contraire, la congruence est impossible évidemment. Admettant donc que b soit divisible par d, la condition imposée à x revient à celle-ci

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \qquad \left[\mathrm{mod}\left(\frac{\mathrm{M}}{d}\right)\right].$$

Puisque $\frac{a}{d}$ et $\frac{\mathrm{M}}{d}$ sont premiers entre eux, nous savons qu'il existe une seule racine par rapport au module $\frac{\mathrm{M}}{d}$. Soit x_0 cette racine, l'ensemble des valeurs de x qui satisfont à la question est comprise dans l'expression

$$x_0 + \frac{\mathrm{M}}{d}y, \qquad y = 0, \ \pm 1, \ \pm 2, \ \pm 3, \ \ldots.$$

Mais il est clair que, suivant le module M, ces nombres se répartissent en *d classes*, car les d nombres

$$x_0, \quad x_0 + \frac{\mathrm{M}}{d}, \quad x_0 + 2\frac{\mathrm{M}}{d}, \quad x_0 + 3\frac{\mathrm{M}}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{\mathrm{M}}{d}$$

sont incongrus suivant le module M, mais un nombre quelconque $x_0 + \frac{\mathrm{M}}{d}y$ est congru, suivant le module M, avec un de ces d nombres.

Théorème I. — *La congruence*

$$ax + b \equiv 0 \qquad (\mathrm{mod}\,\mathrm{M})$$

est possible seulement lorsque b est divisible par $d = (a, \mathrm{M})$. Si cette condition se trouve satisfaite, elle admet exactement d racines.

On voit que cet énoncé renferme aussi le résultat particulier qui a lieu pour $d = 1$.

9. Il nous reste à donner une méthode pour trouver effectivement, sans trop de peine, la racine de la congruence

$$ax + b \equiv 0 \qquad (\mathrm{mod}\,\mathrm{M}).$$

Il est clair que nous pourrons nous borner au cas où a et M sont premiers entre eux, puisque le cas général se ramène immédiatement à ce cas particulier. Ensuite il suffira de considérer la congruence

$$ax \equiv 1 \pmod{M};$$

car, la racine de cette congruence étant obtenue, il suffira évidemment de la multiplier par $-b$ pour obtenir la racine de la congruence proposée. Le problème revient donc à satisfaire à l'équation indéterminée

$$ax - My = 1.$$

On développe en fraction continue le rapport $M:a$ ou, ce qui revient au même, on applique à a et M l'algorithme d'Euclide. On peut alors exprimer de proche en proche comme fonctions linéaires homogènes de a et M tous les restes obtenus et finalement le p. g. c. d. lui-même qui est 1. Comme ce mode de calcul est encore utile dans d'autres circonstances, nous allons l'expliquer avec détails.

Supposons qu'on ait une suite de nombres N, N_1, N_2, ... liés par les relations

$$(1)\qquad \begin{cases} N = a_1 N_1 + N_2, \\ N_1 = a_2 N_2 + N_3, \\ N_2 = a_3 N_3 + N_4, \\ \dots\dots\dots\dots, \\ N_{k-1} = a_k N_k + N_{k+1}, \end{cases}$$

alors on peut exprimer successivement N par N_1 et N_2, par N_2 et N_3, ...,

$$N = a_1 N_1 + N_2,$$
$$N = (a_1 a_2 + 1) N_2 + a_1 N_3,$$
$$N = (a_1 a_2 a_3 + a_1 + a_3) N_3 + (a_1 a_2 + 1) N_4,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$

Introduisons un symbole

$$[a_1, a_2, \dots, a_k],$$

déterminé par les relations

$$(2)\qquad \begin{cases} [a_1] = a_1, \qquad [a_1, a_2] = a_1 a_2 + 1, \\ [a_1, a_2, \dots, a_k] = [a_1, a_2, \dots, a_{k-1}] a_k + [a_1, a_2, \dots, a_{k-2}], \end{cases}$$

alors on aura généralement

$$(3)\qquad N = [a_1, a_2, \dots, a_k] N_k + [a_1, a_2, \dots, a_{k-1}] N_{k+1}.$$

Il est clair qu'on aura aussi

$$N_1 = [a_2, a_3, \ldots, a_k] N_k + [a_2, a_3, \ldots, a_{k-1}] N_{k+1},$$
$$N_2 = [a_3, \ldots, a_k] N_k \quad + [a_3, \ldots, a_{k-1}] N_{k+1},$$

et, si l'on substitue ces valeurs dans la première relation (1), on obtient une expression de N par N_k et N_{k+1} qui doit être identique avec (3). D'où l'on conclut

(4) $$[a_1, a_2, \ldots, a_k] = a_1 [a_2, a_3, \ldots, a_k] + [a_3, \ldots, a_k],$$

ce qui donne un nouveau moyen pour obtenir par récurrence la valeur du symbole. A l'aide de ces relations (2) et (4), on démontrera facilement cette formule

(5) $$[a_1, a_2, \ldots, a_k] = [a_k, a_{k-1}, \ldots, a_2, a_1].$$

En joignant à l'équation (3) celle-ci

(6) $$N_1 = [a_2, a_3, \ldots, a_k] N_k + [a_2, a_3, \ldots, a_{k-1}] N_{k+1},$$

on a deux équations; d'où l'on pourra tirer la valeur de N_k en fonction de N et N_1. Mais cette valeur s'obtient aussi directement, car on obtient de proche en proche

$$-N_2 = N - a_1 N_1,$$
$$-N_3 = a_2 N - [a_1, a_2] N_1,$$
$$+N_4 = [a_2, a_3] N - [a_1, a_2, a_3] N_1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Généralement,

(7) $$(-1)^k N_k = [a_2, a_3, \ldots, a_{k-1}] N - [a_1, a_2, \ldots, a_{k-1}] N_1.$$

En comparant cette valeur de N_k avec celle tirée de (3) et (6), on a

(8) $$[a_1, a_2, \ldots, a_k] \times [a_2, a_3, \ldots, a_{k-1}] - [a_1, a_2, \ldots, a_{k-1}] \times [a_2, a_3, \ldots, a_k] = (-1)^k.$$

Ce sont là les formules dont nous aurons besoin; nous en donnons encore quelques autres qui sont quelquefois utiles. On a

$$N_k \quad = [a_{k+1}, a_{k+2}, \ldots, a_{k+l}] N_{k+l} + [a_{k+1}, \ldots, a_{k+l-1}] N_{k+l+1},$$
$$N_{k+1} = [a_{k+2}, \ldots, a_{k+l}] N_{k+l} \quad + [a_{k+2}, \ldots, a_{k+l-1}] N_{k+l+1}.$$

Substituant ces valeurs dans (3), on a l'expression de N par N_{k+l} et N_{k+l+1}, expression qu'on peut obtenir aussi en remplaçant k par $k+l$ dans la même formule. On trouve, par comparaison,

(9) $$[a_1, a_2, \ldots, a_{k+l}]$$
$$= [a_1, a_2, \ldots, a_k] \times [a_{k+1}, \ldots, a_{k+l}] + [a_1, a_2, \ldots, a_{k-1}] \times [a_{k+2}, \ldots, a_{k+l}].$$

Enfin nous ajouterons la relation suivante

$$(10)\quad \begin{aligned}&[a_1, a_2, \ldots, a_r; b_1, b_2, \ldots, b_s; c_1, c_2, \ldots, c_t] \times [b_1, b_2, \ldots, b_s] \\ &\quad - [a_1, \ldots, a_r; b_1, \ldots, b_s] \times [b_1, \ldots, b_s; c_1, \ldots, c_t] \\ &\quad = (-1)^s [a_1, a_2, \ldots, a_{r-1}] \times [c_2, c_3, \ldots, c_t]\end{aligned}$$

qui, pour $r = t = 1$, reproduit la formule (8) et, pour $s = 0$, la formule (9).

10. Pour appliquer ces relations à la solution de l'équation

$$ax - My = 1,$$

on prendra $N = M$, $N_1 = a$. Comme ces nombres sont premiers entre eux, on finira par trouver $N_k = 1$, $N_{k+1} = 0$, de manière qu'on ait

$$\begin{aligned}M &= [a_1, a_2, \ldots, a_k], \\ a &= [a_2, \ldots, a_k], \\ (-1)^k &= [a_2, a_3, \ldots, a_{k-1}] \times M - [a_1, a_2, \ldots, a_{k-1}] \times a.\end{aligned}$$

On peut donc prendre

$$\begin{aligned}x &= (-1)^{k-1}[a_1, a_2, \ldots, a_{k-1}], \\ y &= (-1)^{k-1}[a_2, a_3, \ldots, a_{k-1}].\end{aligned}$$

Si l'on fait le calcul de la manière ordinaire, le dernier quotient a_k est au moins égal à 2, et l'on peut le remplacer par les deux quotients $a_k - 1$ et 1, de manière que le nombre total des quotients est à volonté pair ou impair. Il est à peine besoin de dire que

$$\frac{M}{a} = \frac{[a_1, a_2, \ldots, a_k]}{[a_2, a_3, \ldots, a_k]} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_k}}}.$$

On voit sans peine que, x_0, y_0 étant une solution particulière de

$$ax - My = 1,$$

la solution la plus générale sera renfermée dans les formules

$$\left.\begin{aligned}x &= x_0 - Mt \\ y &= y_0 - at\end{aligned}\right\} \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

Il est clair aussi que l'équation indéterminée

$$ax + by = c$$

sera impossible si c n'est pas divisible par $d = (a, b)$. Mais, si cette condition est satisfaite, il y a toujours une infinité de solutions. Soit x_0, y_0 une solution particulière, la solution la plus générale sera

$$\left.\begin{aligned} x &= x_0 + \frac{b}{d}t \\ y &= y_0 - \frac{a}{d}t \end{aligned}\right\} \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

11. Nous allons considérer maintenant le problème suivant, qui se rencontre très souvent :

Trouver tous les nombres x qui satisfont au système suivant de n congruences

$$x \equiv \alpha \pmod{A}, \quad x \equiv \beta \pmod{B}, \quad x \equiv \gamma \pmod{C}, \quad \ldots, \quad x \equiv \lambda \pmod{L}.$$

Soit M le p. p. c. m. des modules A, B, C, ..., L, il est clair que, si la valeur $x = x_0$ satisfait aux conditions, il en sera de même de toutes celles comprises dans la formule

$$x_0 + Mt \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

Réciproquement, si l'on a deux solutions x_0 et x_1, la différence $x_0 - x_1$ doit être divisible par M, puisqu'elle est divisible par A, par B, ..., par L. Il résulte de là que, parmi les nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M - 1$$

formant un système complet de résidus pour le module M, il y en aura tout au plus un qui satisfait aux conditions, et nous pouvons dire :

Si le problème proposé admet des solutions, ces solutions seront toutes renfermées dans la formule

$$x \equiv a \pmod{M},$$

où a est un nombre déterminé de la série $0, 1, \ldots, M - 1$.

Mais, si aucun des nombres $0, 1, \ldots, M - 1$ ne satisfait au problème, on sera assuré que le problème est impossible et n'admet aucune solution.

Supposons maintenant d'abord que A, B, C, ..., L soient premiers entre eux, alors $M = ABC \ldots L$. Si l'on divise maintenant chacun des nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M - 1$$

par A, par B, ..., par L, on obtiendra en tout M systèmes de résidus qui seront tous différents. Mais, d'autre part, on ne peut donner à α que A valeurs, à β B valeurs, etc., en sorte que le nombre total des systèmes de résidus possibles est M.

En divisant donc les nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1$$

par A, B, C, ..., L, on obtiendra effectivement tous les systèmes possibles de résidus, et chaque système une seule fois.

THÉORÈME II. — *Les modules* A, B, C, ..., L *étant premiers entre eux, le système des congruences*

$$x \equiv \alpha \pmod{A}, \qquad x \equiv \beta \pmod{B}, \qquad \ldots, \qquad x \equiv \lambda \pmod{L}$$

admet toujours des solutions, renfermées toutes dans la formule

$$x \equiv a \pmod{M},$$

où

$$M = ABC\ldots L.$$

12. Lorsque les modules A, B, C, ..., L ne sont pas premiers entre eux, M est plus petit que le produit ABC...L.

Or il y a toujours ABC...L systèmes de résidus possibles (si l'on prend $\alpha, \beta, \gamma, \ldots, \lambda$ arbitrairement). Mais le problème ne sera possible que si le système $\alpha, \beta, \gamma, \ldots, \lambda$ se trouve parmi les M systèmes de résidus qu'on obtient en divisant les nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1$$

par A, B, C, ..., L. On voit donc que, dans ce cas, le problème ne sera pas possible toujours : il faudra, pour cela, que $\alpha, \beta, \ldots, \lambda$ satisfassent à certaines conditions que nous énoncerons plus bas. Mais toujours, lorsque le problème est possible, la solution est donnée par une formule

$$x \equiv a \pmod{M}.$$

13. Revenons au cas où A, B, C, ..., L sont premiers entre eux pour voir comment on obtiendra la solution $x \equiv a \pmod{M}$.

Puisqu'on doit avoir $x \equiv \alpha \pmod{A}$, on posera

$$x = \alpha + Ay,$$

et il viendra

$$Ay \equiv \beta - \alpha \pmod{B},$$

$$Ay \equiv \gamma - \alpha \pmod{C}.$$

La première congruence donnera

$$y = y_0 + Bz,$$

on substituera cette valeur dans les autres congruences, etc.

On remplacera cette méthode souvent avec avantage par la suivante indiquée par Gauss.

Déterminons d'abord les nombres auxiliaires α', β', ..., λ' par les congruences

$$\begin{aligned}
\text{BCD}\ldots\text{L}\alpha' &\equiv 1 \pmod{\text{A}},\\
\text{ACD}\ldots\text{L}\beta' &\equiv 1 \pmod{\text{B}},\\
\text{ABD}\ldots\text{L}\gamma' &\equiv 1 \pmod{\text{C}},\\
&\ldots\ldots\\
\text{AB}\ldots\text{K}\lambda' &\equiv 1 \pmod{\text{L}},
\end{aligned}$$

alors on aura

$$\begin{aligned}
x \equiv\ & \text{BCD}\ldots\text{L}\alpha\alpha'\\
&+ \text{ACD}\ldots\text{L}\beta\beta'\\
&+ \text{ABD}\ldots\text{L}\gamma\gamma'\\
&\ldots\ldots\ldots\ldots\\
&+ \text{ABC}\ldots\text{K}\lambda\lambda' \qquad (\text{mod}\,\text{M} = \text{ABC}\ldots\text{L}).
\end{aligned}$$

On vérifie, en effet, immédiatement que cette valeur de x satisfait aux congruences proposées, et il est facile de s'apercevoir que cette méthode revient à résoudre la question successivement dans les cas particuliers où l'un des résidus α, β, ..., λ est 1 et où tous les autres sont 0. On compose ensuite la solution générale avec ces solutions particulières. Il est clair que cette méthode sera surtout avantageuse lorsqu'on aura à résoudre le même système pour diverses valeurs des résidus α, β, ..., λ, les modules A, B, ..., L restant les mêmes. Les mêmes nombres α', β', ..., λ' servent alors pour les diverses solutions.

14. Revenons maintenant au cas général où les modules A, B, ..., L ne sont pas premiers entre eux. On peut d'abord poser comme tout à l'heure

$$x = \alpha + \text{A}y,$$

et la seconde congruence deviendra

$$\text{A}y \equiv \beta - \alpha \pmod{\text{B}}.$$

Il faudra donc que $\beta - \alpha$ soit divisible par $(\text{A}, \text{B}) = d$. Si cette condition n'est pas satisfaite, le système n'admet aucune solution. Mais, si elle est satisfaite, on aura

$$y = y_0 + \frac{\text{B}}{d}t \qquad (t = 0, \pm 1, \pm 2, \ldots)$$

et, par conséquent,

$$x \equiv \alpha + \text{A}y_0 \quad \left(\text{mod}\,\frac{\text{AB}}{d}\right),$$

et cette congruence remplace maintenant les deux premières $x \equiv \alpha \pmod{A}$, $x \equiv \beta \pmod{B}$. On remarquera que le module $\frac{AB}{d}$ est bien le p. p. c. m. de A et B.

On pourra combiner maintenant la congruence

$$x \equiv \alpha + Ay_0 \qquad \left(\bmod \frac{AB}{d}\right)$$

avec la troisième

$$x \equiv \gamma \qquad (\bmod C),$$

et ainsi de suite. Il est clair qu'on arrivera de cette façon toujours, soit à s'assurer que le problème est impossible, soit à trouver la solution sous la forme

$$x \equiv a \qquad (\bmod M)$$

si elle existe.

Cette méthode, toutefois, a l'inconvénient de ne faire souvent connaître l'impossibilité du problème qu'après de longs calculs qui ont été inutiles alors. On ne peut remédier à cet inconvénient qu'en donnant le moyen de reconnaître *a priori* la possibilité ou l'impossibilité du problème. C'est là l'objet du théorème suivant :

Théorème III. — *Pour que le système des congruences*

$$x \equiv \alpha \quad (\bmod A), \qquad x \equiv \beta \quad (\bmod B), \qquad \ldots, \qquad x \equiv \lambda \quad (\bmod L)$$

admette des solutions, il faut et il suffit que les différences

$$\alpha - \beta, \quad \alpha - \gamma, \quad \beta - \gamma, \quad \ldots, \quad \alpha - \lambda$$

soient divisibles respectivement par

$$(A, B), \quad (A, C), \quad (B, C), \quad \ldots, \quad (K, L).$$

Que ces conditions sont nécessaires, cela est clair d'après ce qui précède. Pour montrer qu'elles sont suffisantes, nous supposerons que la proposition est exacte dans le cas de $n-1$ congruences, et ferons voir qu'elle est alors exacte aussi dans le cas de n congruences. Puisqu'on sait que, dans le cas $n = 2$, le théorème est vrai, il sera ainsi démontré généralement.

En effet, la proposition étant vraie pour $n-1$ congruences, on pourra remplacer les $n-1$ premières congruences par celle-ci

$$x \equiv t \qquad (\bmod M')$$

et le système complet par

(1) $$x \equiv t \quad (\bmod M'), \qquad x \equiv \lambda \quad (\bmod L).$$

Ici $M' = \{A, B, C, \ldots, K\}$. Or, d'après notre hypothèse,

$$\lambda - \alpha, \quad \lambda - \beta, \quad \ldots, \quad \lambda - \chi$$

sont divisibles par

$$(L, A), \quad (L, B), \quad \ldots, \quad (L, K)$$

respectivement, et il est clair que

$$\alpha - t, \quad \beta - t, \quad \ldots, \quad \chi - t$$

sont divisibles par $A, B, C, \ldots, K$ respectivement, donc aussi par (L, A), $(L, B), \ldots, (L, K)$ respectivement. On voit par là que la différence

$$\lambda - t$$

est divisible par (L, A), par $(L, B), \ldots$, par (L, K) et, par conséquent, aussi par le p. p. c. m. de ces nombres qui est (L, M') (Chap. I, n° 11). Mais cette divisibilité de $\lambda - t$ par (L, M') est précisément la condition nécessaire et suffisante pour que les congruences (1) et par là aussi les congruences proposées admettent une solution.

On peut démontrer ce théorème aussi en faisant voir qu'il y a exactement M systèmes de résidus $\alpha, \beta, \ldots, \lambda$ qui satisfont aux conditions exigées.

15. On peut réduire le cas général au cas où $A, B, \ldots, L$ sont premiers entre eux. Pour cela, mettons le p. p. c. m. M des modules sous la forme

$$M = A'B'C'\ldots L',$$

où $A', B', C', \ldots, L'$ sont premiers entre eux et divisent respectivement $A, B, C, \ldots, L$ (Chap. I, n°s 18, 19).

Il est clair que les solutions du problème proposé satisferont aussi aux congruences

$$x \equiv \alpha \pmod{A'}, \qquad x \equiv \beta \pmod{B'}, \qquad \ldots, \qquad x \equiv \lambda \pmod{L'},$$

mais ce dernier système admet, nous le savons, toujours des solutions renfermées dans la formule

$$x \equiv a \pmod{M}.$$

Si donc on s'est assuré préalablement que le problème proposé admet des solutions, ces solutions sont encore renfermées dans la formule précédente. Mais, si l'on ne savait pas si oui ou non le système proposé admet des solutions, cette valeur $x \equiv a \pmod{M}$ pourrait ne pas satisfaire aux conditions imposées, qui seraient alors incompatibles.

Considérons, par exemple, le système

$$
\begin{aligned}
x &\equiv 31 \quad (\text{mod } 72 = 2^3.3^2),\\
x &\equiv 22 \quad (\text{mod } 105 = 3.5.7),\\
x &\equiv 50 \quad (\text{mod } 77 = 7.11),\\
x &\equiv 337 \quad (\text{mod } 399 = 3.7.19).
\end{aligned}
$$

On a ici $M = 2^3.3^2.5.7.11.19 = 526680$ et $ABCD : M = 441$. Donc, si les résidus 31, 22, 50, 337 avaient été pris au hasard, il n'y aurait qu'une chance sur 441 que le problème soit possible. Il convient donc de s'assurer d'abord si le problème est possible ou non. Or, les nombres

$$9, \quad 19, \quad 306, \quad 28, \quad 315, \quad 287$$

étant divisibles respectivement par

$$3, \quad 1, \quad 3, \quad 7, \quad 21, \quad 7,$$

le problème est possible. La décomposition de M

$$M = 72 \times 35 \times 11 \times 19$$

permet maintenant de remplacer les congruences données par celles-ci

$$
\begin{aligned}
x &\equiv 31 && (\text{mod } 72),\\
x &\equiv 22 && (\text{mod } 35),\\
x &\equiv 50 \equiv 6 && (\text{mod } 11),\\
x &\equiv 337 \equiv 14 && (\text{mod } 19).
\end{aligned}
$$

En appliquant maintenant la méthode de Gauss, les nombres auxiliaires α', β', γ', δ' se déterminent par les congruences

$$
\begin{aligned}
35.11.19\,\alpha' &\equiv 43\,\alpha' \equiv 1 && (\text{mod } 72),\\
72.11.19\,\beta' &\equiv -2\beta' \equiv 1 && (\text{mod } 35),\\
72.35.19\,\gamma' &\equiv 8\gamma' \equiv 1 && (\text{mod } 11),\\
72.35.11\,\delta' &\equiv -\delta' \equiv 1 && (\text{mod } 19),
\end{aligned}
$$

d'où

$$\alpha' = -5, \qquad \beta' = 17, \qquad \gamma' = 7, \qquad \delta' = -1,$$

et, finalement,

$$
\begin{aligned}
x \equiv &- 5.35.11.19.31\\
&+ 17.72.11.19.22 \qquad (\text{mod } 526\,680),\\
&+ 7.72.35.19.6\\
&- 72.35.11.14
\end{aligned}
$$

$$x \equiv 323\,527 \qquad (\text{mod } 526\,680),$$

16. Soient

$$\alpha,\quad \alpha',\quad \alpha'',\quad \ldots$$

les $\varphi(a)$ nombres premiers avec a et ne surpassant pas a,

$$\beta,\quad \beta',\quad \beta'',\quad \ldots$$

les $\varphi(b)$ nombres premiers avec b et ne dépassant pas b,

$$\gamma,\quad \gamma',\quad \gamma'',\quad \ldots$$

les $\varphi(ab)$ nombres premiers avec ab et ne surpassant pas ab. Il est clair que tout nombre γ est aussi premier avec a et avec b, et sera par conséquent congru avec un des nombres α suivant le module a, et congru avec un des nombres β suivant le module b. Mais, si nous supposons maintenant a et b premiers entre eux, nous savons aussi qu'en prenant arbitrairement un des nombres α et un des nombres β, il y a toujours au-dessous de ab un nombre et un seul qui leur sera congru suivant les modules a et b, respectivement; et ce nombre, étant premier avec a et avec b, sera premier avec ab et figurera donc parmi les nombres γ. Ensuite deux nombres γ, γ' donnant toujours deux systèmes de résidus différents, on conclut

$$\varphi(ab) = \varphi(a)\varphi(b).$$

C'est la relation que nous avons déjà rencontrée (n° 6) et qui conduit immédiatement à la détermination de la fonction φ, car on voit facilement que

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

17. Considérons maintenant une congruence quelconque

$$(1)\qquad f(x) \equiv 0 \pmod{M},$$

et supposons

$$M = ABC\ldots L,$$

les facteurs A, B, C, ..., L étant premiers entre eux.

Il est clair que chaque racine de la congruence (1) satisfera aussi aux congruences

$$(2)\qquad \begin{cases} f(x) \equiv 0 \pmod{A}, \\ f(x) \equiv 0 \pmod{B}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f(x) \equiv 0 \pmod{L}. \end{cases}$$

Donc, si une de ces dernières congruences n'admet pas de racines, il en est de même de la congruence (1).

Soient α une racine de $f(x) \equiv 0 \pmod{A}$, β une racine de $f(x) \equiv 0 \pmod{B}$, etc., enfin λ une racine de $f(x) \equiv 0 \pmod{L}$.

Alors on saura trouver toujours un nombre t, satisfaisant aux congruences

$$\begin{aligned} t &\equiv \alpha \pmod{A}, \\ t &\equiv \beta \pmod{B}, \\ &\ldots\ldots\ldots\ldots \\ t &\equiv \lambda \pmod{L}, \end{aligned}$$

et ce nombre t est parfaitement déterminé aux multiples de M près.

Mais il est clair qu'on aura

$$f(t) \equiv 0 \pmod{A}, \quad f(t) \equiv 0 \pmod{B}, \quad \ldots, \quad f(t) \equiv 0 \pmod{L};$$

donc aussi $f(t) \equiv 0 \pmod{M}$.

On conclut de là que le nombre des solutions de la congruence (1) est égal au produit des nombres des solutions des congruences (2).

On peut évidemment prendre pour A, B, ..., L des puissances de nombres premiers.

18. On comprend bien, d'après ce qui précède, que dans la théorie des congruences de degré supérieur, on s'est surtout occupé des cas où le module est un nombre premier ou une puissance de nombre premier. On ne connaît presque aucun théorème général sur les congruences par rapport à un module composé.

Ici, où il s'agit seulement de donner les premiers éléments d'une théorie que nous devons développer plus tard, nous nous bornerons à considérer le cas d'un module premier. Lagrange a obtenu dans ce cas quelques propositions très simples, mais fondamentales.

Considérons donc la congruence

$$f(x) \equiv 0 \pmod{p},$$

p étant un nombre premier. Le degré n de cette congruence est le degré de la plus haute puissance de x qui figure dans $f(x)$, avec un coefficient non divisible par p. Du reste, il n'y aurait aucun inconvénient à supposer ce coefficient égal à 1, car, s'il est a, on pourra toujours multiplier la congruence par un nombre b tel que $ab \equiv 1 \pmod{p}$. La congruence obtenue est évidemment équivalente à la congruence proposée.

Soit maintenant $x = \alpha$ une racine de la congruence. En divisant $f(x)$ par $x - \alpha$, on aura

$$f(x) = (x - \alpha) f_1(x) + f(\alpha),$$

$f_1(x)$ étant un polynôme du degré $n - 1$ à coefficients entiers.

La congruence donnée peut donc s'écrire

$$(x-\alpha)f_1(x)+f(\alpha)\equiv 0 \pmod{p},$$

ou bien, puisque par hypothèse $f(\alpha)$ est divisible par p,

$$(x-\alpha)f_1(x)\equiv 0 \pmod{p}.$$

Si la congruence proposée admet encore d'autres racines β, γ, ..., on doit avoir

$$\begin{aligned}(\beta-\alpha)f_1(\beta)&\equiv 0,\\ (\gamma-\alpha)f_1(\gamma)&\equiv 0,\\ \ldots\ldots&\ldots\ldots;\end{aligned}$$

donc $f_1(\beta)\equiv 0$, $f_1(\gamma)\equiv 0$, etc., puisque, par hypothèse, $\beta-\alpha$, $\gamma-\alpha$ ne sont pas divisibles par p. On voit donc que ces racines β, γ, ... sont aussi racines de la congruence

$$f_1(x)\equiv 0$$

qui est du degré $n-1$.

La congruence du premier degré admet toujours *une* racine : on peut donc conclure qu'une congruence du second degré admet tout au plus 2 racines, une congruence du troisième degré tout au plus 4 racines; généralement on peut énoncer le

Théorème IV. — *Une congruence de degré n par rapport à un module premier admet tout au plus n racines.*

Et nous pouvons ajouter encore :

Théorème V. — *Les racines de la congruence de degré n*

$$f(x)\equiv 0 \pmod{p}$$

étant α, β, γ, ..., λ, on a identiquement

$$f(x)\equiv(x-\alpha)(x-\beta)\ldots(x-\lambda)f_1(x) \pmod{p}.$$

$f_1(x)$ étant un polynôme en x tel que la congruence

$$f_1(x)\equiv 0 \pmod{p}$$

n'admet aucune racine.

On en déduit encore facilement le

Théorème VI. — *Si la congruence de degré n*

$$f(x)\equiv 0 \pmod{p}$$

admet n racines et qu'on a

$$f(x) \equiv f_1(x) f_2(x) \pmod{p},$$

alors les congruences

$$f_1(x) \equiv 0, \qquad f_2(x) \equiv 0 \pmod{p}$$

des degrés n_1 et n_2 $(n_1 + n_2 = n)$ admettront respectivement n_1 et n_2 racines.

19. Pour donner, dès à présent, un exemple de la fécondité de ces principes, considérons avec Lagrange le polynôme

$$(1) \qquad x(x+1)(x+2)\ldots(x+p-1) = x^p + A_1 x^{p-1} + A_2 x^{p-2} + \ldots + A_{p-1} x.$$

En changeant x en $x+1$, on aura aussi

$$(x+1)(x+2)\ldots(x+p) = (x+1)^p + A_1(x+1)^{p-1} + A_2(x+p)^{p-2} + \ldots + A_{p-1}(x+1).$$

Or, il est clair que ces deux polynômes sont congrus entre eux suivant le module p, que nous supposerons premier, car leur différence est

$$p(x+1)(x+2)\ldots(x+p-1).$$

En écrivant donc que les coefficients des mêmes puissances de x sont congrus $(\bmod p)$, on a

$$A_1 \equiv \frac{p}{1} + A_1 \pmod{p},$$

$$A_2 \equiv \frac{p(p-1)}{1.2} + \frac{p-1}{1} A_1 + A_2,$$

$$A_3 \equiv \frac{p(p-1)(p-2)}{1.2.3} + \frac{(p-1)(p-2)}{1.2} A_1 + \frac{p-2}{1} A_2 + A_3,$$

....

$$A_{p-1} \equiv \frac{p(p-1)\ldots 3.2}{1.2\ldots(p-1)} + \frac{(p-1)\ldots 2}{1.2.(p-2)} A_1 + \ldots + \frac{2}{1} A_{p-2} + A_{p-1},$$

$$0 \equiv 1 + A_1 + A_2 + \ldots + A_{p-2} + A_{p-1}.$$

On remarque ici que les coefficients du binôme $\frac{p}{1}, \frac{p(p-1)}{1.2} \ldots \frac{p(p-1)\ldots 3.2}{1.2\ldots(p-1)}$ sont tous des entiers divisibles par p : on peut les négliger. La seconde congruence montre alors que $A_1 \equiv 0 \bmod p$, ensuite la troisième que $A_2 \equiv 0 \bmod p$, etc., jusqu'à l'avant-dernière, qui montre que $A_{p-2} \equiv 0$. Donc

$$(2) \qquad A_1 \equiv A_2 \equiv A_3 \equiv \ldots \equiv A_{p-2} \equiv 0 \pmod{p}$$

et la dernière congruence donne ensuite

$$(3) \qquad A_{p-1}+1 \equiv 0 \pmod{p}.$$

Si l'on se rappelle la signification de A_{p-1}, on a le

Théorème de Wilson, *p étant un nombre premier,*

$$1.2.3\ldots(p-1)+1$$

est toujours divisible par p.

Ensuite nous avons d'après (1), (2) et (3) la congruence identique

$$x(x+1)(x+2)\ldots\quad(x+p-1) \equiv x^p - x \pmod{p}.$$

Mais, parmi les p nombres consécutifs $x, x+1, \ldots, x+p-1$, il y en a toujours un divisible par p; donc

$$x^p - x$$

est toujours divisible par p. En supposant $x = a$ non divisible par p, on a le

Théorème de Fermat. — *a étant un nombre entier non divisible par le nombre premier p,*

$$a^{p-1}-1$$

est toujours divisible par p.

Autrement, la congruence $x^{p-1}-1 \equiv 0 \pmod{p}$ admet les $p-1$ racines $1, 2, 3 \ldots p-1$.

Le théorème de Fermat est un des théorèmes les plus importants de la théorie des nombres; nous le retrouverons dans le Chapitre IV, où nous traiterons particulièrement des résidus des puissances et de la théorie des congruences binômes.

20. Les systèmes de plusieurs congruences du premier degré à plusieurs inconnues se présentent maintenant naturellement à notre attention, mais nous consacrerons à ce sujet important le Chapitre III tout entier. Ici nous nous bornerons à traiter une question élémentaire et dont on a souvent besoin. La théorie des équations indéterminées est liée évidemment très étroitement à la théorie des congruences; nous discuterons ici l'équation indéterminée

$$(1) \qquad a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_{n+1}x_{n+1} = u,$$

$a_1, a_2, \ldots, a_{n+1}$ et u étant des nombres donnés, $x_1, x_2, \ldots, x_{n+1}$ étant des inconnues qui doivent avoir des valeurs entières. Il est clair d'abord que u doit être

divisible par le p. g. c. d.

$$d = (a_1, a_2, \ldots, a_{n+1})$$

des coefficients $a_1, a_2, \ldots, a_{n+1}$.

Mais, pour que d ait une valeur déterminée, il faut supposer que les coefficients $a_1, a_2, \ldots, a_{n+1}$ ne soient pas tous nuls. Ce sera là la seule restriction à laquelle nous soumettons les données du problème. Maintenant, si u est divisible par d, le problème admet toujours des solutions. Cette proposition est vraie dans le cas $n = 1$, et il est très facile, en partant de là, et à l'aide d'une induction, de montrer qu'elle est vraie généralement.

Mais nous suivrons une autre voie qui nous donnera en même temps toutes les solutions du problème. Mais ici une explication est nécessaire, si les valeurs

$$x_1 = b_1, \quad x_2 = b_2, \quad \ldots, \quad x_{n+1} = b_{n+1},$$

satisfont à la relation (1); de même que les valeurs

$$x_1 = c_1, \quad x_2 = c_2, \quad \ldots, \quad x_{n+1} = c_{n+1},$$

ces deux solutions seront considérées comme distinctes si les différences

$$b_k - c_k, \qquad k = 1, 2, \ldots, n+1$$

ne sont pas toutes nulles. Il importe de bien observer cette convention; ainsi, même dans le cas où $a_{n+1} = 0$, les solutions

$$x_1 = b_1, \quad x_2 = b_2, \quad \ldots, \quad x_n = b_n, \quad x_{n+1} = b_{n+1}$$

et

$$x_1 = b_1, \quad x_2 = b_2, \quad \ldots, \quad x_n = b_n, \quad x_{n+1} = b_{n+1} + k$$

seront considérées comme distinctes, tant que k n'est pas nul.

Les coefficients $a_1, \ldots, a_{n+1}$ n'étant pas tous nuls, on supposera que a_1 n'est pas nul. On pourra déterminer alors deux nombres α et γ satisfaisant à la condition

$$a_1\alpha + a_2\gamma = (a_1, a_2).$$

et ces nombres seront premiers entre eux, en sorte qu'on pourra ensuite déterminer deux nombres β et δ par la condition

$$\alpha\delta - \beta\gamma = 1.$$

On pourra prendre du reste $\beta = -a_2 : (a_1, a_2)$, $\delta = +a_1 : (a_1, a_2)$; c'est là une remarque dont nous profiterons tout à l'heure.

Posons

$$\left.\begin{aligned} x_1 &= \alpha x'_1 + \beta x'_2, \\ x_2 &= \gamma x'_1 + \delta x'_2, \end{aligned}\right\} \quad \text{d'où} \quad \left\{\begin{aligned} x'_1 &= \delta x_1 - \beta x_2, \\ x'_2 &= -\gamma x_1 + \alpha x_2, \end{aligned}\right.$$

l'équation (1) deviendra

$$(2) \qquad (a_1, a_2)x'_1 + b_2 x'_2 + a_3 x_3 + a_4 x_4 + \ldots + a_{n+1} x_{n+1} = u.$$

Il est clair que ces équations (1) et (2) sont équivalentes en ce sens, que si l'une des équations est impossible, l'autre le sera; et que, si l'on connaît une solution de l'une de ces équations, on en déduira une solution de l'autre. A deux solutions distinctes d'une de ces équations correspondent toujours deux solutions également distinctes de l'autre.

Remplaçons maintenant de la même manière les inconnues x'_1 et x_3 dans (2) par deux nouvelles inconnues x''_1 et x'_3, en posant

$$\begin{gathered} (a_1, a_2)\alpha_1 + a_3\gamma_1 = (a_1, a_2, a_3), \\ \alpha_1\delta_1 - \beta_1\gamma_1 = 1, \\ x'_1 = \alpha_1 x''_1 + \beta_1 x'_3, \qquad x''_1 = \delta_1 x'_1 - \beta_1 x_3, \\ x_3 = \gamma_1 x''_1 + \delta_1 x'_3, \qquad x'_3 = -\gamma_1 x'_1 + \alpha_1 x_3, \end{gathered}$$

on obtiendra une transformée encore équivalente à (2) et à (1)

$$(3) \qquad (a_1, a_2, a_3)x''_1 + b_2 x'_2 + b_3 x'_3 + a_4 x_4 + \ldots + a_{n+1} x_{n+1} = u.$$

On peut continuer ainsi, en opérant maintenant sur x''_1 et x_4, etc. Après n transformations, on aura la transformée équivalente que voici

$$(4) \qquad (a_1, a_2, \ldots, a_{n+1})x_1^{(n)} + b_2 x'_2 + b_3 x'_3 + b_4 x'_4 + \ldots + b_{n+1} x'_{n+1} = u.$$

et l'on obtient les expressions de $x_1, \ldots, x_{n+1}$ au moyen de substitutions successives sous la forme

$$(5) \quad \left\{\begin{aligned} x_1 &= A_1 x_1^{(n)} + a_{1,2} x'_2 + a_{1,3} x'_3 + a_{1,4} x'_4 + \ldots + a_{1,n+1} x'_{n+1}, \\ x_2 &= A_2 x_1^{(n)} + a_{2,2} x'_2 + a_{2,3} x'_3 + a_{2,4} x'_4 + \ldots + a_{2,n+1} x'_{n+1}, \\ x_3 &= A_3 x_1^{(n)} \qquad\qquad + a_{3,3} x'_3 + a_{3,4} x'_4 + \ldots + a_{3,n+1} x'_{n+1}, \\ x_4 &= A_4 x_1^{(n)} \qquad\qquad\qquad\qquad + a_{4,4} x'_4 + \ldots + a_{4,n+1} x'_{n+1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_{n+1} &= A_{n+1} x_1^{(n)} \qquad\qquad\qquad\qquad\qquad\qquad + a_{n+1,n+1} x'_{n+1}. \end{aligned}\right.$$

Ces formules donneront toutes les solutions du problème, si l'on prend pour $x_1^{(n)}, x'_2, x'_3, \ldots, x'_{n+1}$ toutes les solutions de (4). Mais on remarque que, si l'on prend pour β et δ les valeurs que nous avons indiquées plus haut, on a $b_2 = 0$.

En appliquant donc toujours le même procédé, on aura aussi

$$b_3 = b_4 = \ldots = b_{n+1} = 0.$$

Mais alors les solutions de (4) sont en évidence; il faut évidemment que u soit divisible par d, et l'on obtient toutes les solutions de (4) en prenant $x_1^{(n)} = u : d$, et en donnant à

$$x'_2, \quad x'_3, \quad \ldots, \quad x'_{n+1}$$

toutes les valeurs de $-\infty$ à $+\infty$.

Théorème VII. — *On obtient toutes les solutions de l'équation indéterminée* (1), *et chaque solution, une seule fois, en posant $x_1^{(n)} = u : d$ dans les formules* (5) *et en faisant parcourir à $x'_2, \ldots, x'_{n+1}$ toutes les valeurs entières de $-\infty$ à $+\infty$.*

On voit sans difficulté qu'en procédant comme nous l'avons indiqué, les coefficients $a_{22}, a_{33}, \ldots, a_{n+1,n+1}$ ont les valeurs suivantes :

$$a_{2,2} = a_1 : (a_1, a_2),$$
$$a_{3,3} = (a_1, a_2) : (a_1, a_2, a_3),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{n+1,n+1} = (a_1, a_2, \ldots, a_n) : (a_1, a_2, \ldots, a_{n+1}).$$

21. Cette solution donne lieu à quelques remarques utiles. Il est clair qu'en ajoutant les équations (5) après les avoir multipliées par $a_1, a_2, \ldots, a_{n+1}$ les coefficients de $x'_2, x'_3, \ldots, x'_{n+1}$, s'annulent. On a ainsi des relations homogènes entre $a_1, a_2, \ldots, a_{n+1}$, qui déterminent les rapports de ces quantités. En supposant

$$D = \begin{vmatrix} X_1 & X_2 & X_3 & \ldots & X_{n+1} \\ a_{1,2} & a_{2,2} & 0 & \ldots & 0 \\ a_{1,3} & a_{2,3} & a_{3,3} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & . \\ a_{1,n+1} & a_{2,n+1} & a_{3,n+1} & \ldots & a_{n+1,n+1} \end{vmatrix} = M_1 X_1 + M_2 X_2 + \ldots + M_{n+1} X_{n+1},$$

on aura

$$a_1 : a_2 : a_3 : \ldots : a_{n+1} = M_1 : M_2 : M_3 : \ldots : M_{n+1}.$$

Mais il est clair qu'on a

$$M_1 = a_{2,2} \times a_{3,3} \times \ldots \times a_{n+1,n+1} = a_1 : d;$$

donc, généralement,

$$M_k = a_k : d. \qquad k = 1, 2, \ldots, n+1$$

En multipliant donc, par exemple, la dernière ligne horizontale du déterminant D par d, on obtient un déterminant dont les mineurs ont les valeurs a_1, a_2, ..., a_{n+1}. On voit par là *que l'on peut toujours déterminer n lignes de $n+1$ nombres entiers telles qu'en ajoutant une $(n+1)^{\text{ième}}$ ligne et formant le déterminant, les coefficients multipliés dans ce déterminant par les différents termes de la $(n+1)^{\text{ième}}$ ligne, soient des nombres donnés.*

C'est là une proposition donnée par M. Hermite (*Journal de Crelle*, t. 40, p. 264), qui en a fait une application très importante.

22. En cherchant l'expression de $x_1^{(n)}$, x'_2, ..., x'_{n+1} comme fonctions linéaires de x_1, x_2, ..., x_{n+1}, on trouve d'abord, à cause de $b_2 = b_3 = \ldots = b_{n+1} = 0$,

$$(a_1, a_2)\, x'_1 = a_1 x_1 + a_2 x_2,$$
$$(a_1, a_2, a_3)\, x''_1 = a_1 x_1 + a_2 x_2 + a_3 x_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$(a_1, a_2, \ldots, a_{n+1})\, x_1^{(n)} = a_1 x_1 + a_2 x_2 \ldots + a_{n+1} x_{n+1},$$

et ensuite on reconnaît que les expressions cherchées se présentent sous la forme

$$x_1^{(n)} = (a_1 x_1 + a_2 x_1 + \ldots + a_{n+1} x_{n+1}) : d,$$
$$x'_2 = \alpha_{2,1} x_1 + \alpha_{2,2} x_2,$$
$$x'_3 = \alpha_{3,1} x_1 + \alpha_{3,2} x_2 + \alpha_{3,3} x_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x'_{n+1} = \alpha_{n+1,1} x_1 + \alpha_{n+2,2} x_2 + \ldots + \alpha_{n+1,n+1} x_{n+1}.$$

Le déterminant des fonctions linéaires au second membre est évidemment $= 1$, comme cela a lieu pour les équations (5), car les déterminants des deux systèmes sont réciproques et en même temps des nombres entiers. Ces déterminants sont donc, tous les deux, soit $= +1$, soit $= -1$, mais il est facile de voir que c'est la première valeur qui a lieu.

On voit donc que, étant donnés les nombres entiers

$$a_1, \quad a_2, \quad \ldots, \quad a_{n+1},$$

on pourra trouver toujours n lignes de $n+1$ nombres entiers, telles qu'en les ajoutant à la ligne donnée, on obtient un déterminant égal au p. g. c. d. de a_1, a_2, ..., a_{n+1}.

C'est là un résultat dont on a souvent besoin. La question a été posée et résolue par M. Hermite (*Journal de Mathématiques appliquées*, t. XIV, 1849). Nous verrons, dans le Chapitre III, qu'il est extrêmement facile de déduire d'une solution particulière de ce problème toutes les solutions possibles.

23. Il convient de considérer plus particulièrement le cas $u = 0$,

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_{n+1}x_{n+1} = 0.$$

Si l'on a m solutions de cette équation

$$\begin{matrix} k_{1,1} & k_{1,2} & k_{1,3} & \ldots & k_{1,n+1} & (\mathrm{K}_1) \\ k_{2,1} & k_{2,2} & k_{2,3} & \ldots & k_{2,n+1} & (\mathrm{K}_2) \\ \ldots & \ldots & \ldots & \ldots & \ldots\ldots & \ldots\ldots \\ k_{m,1} & k_{m,2} & k_{m,3} & \ldots & k_{m,n+1} & (\mathrm{K}_n) \end{matrix}$$

nous dirons que ces solutions sont *indépendantes*, lorsque les déterminants de degré m dont les éléments sont puisés dans cette matrice (et que nous appellerons les déterminants de ces solutions) ne sont pas tous nuls. Il est clair qu'un système de solutions indépendantes se composera tout au plus de n solutions, car, les nombres a_1, a_n, $\ldots$, a_{n+1} n'étant pas tous nuls, le déterminant de $n+1$ solutions est toujours nul. On peut représenter une solution par un simple symbole (K_1) qui représente ainsi $n+1$ nombres entiers, pris dans un ordre déterminé.

On peut déduire des solutions (K_1), (K_2), $\ldots$, (K_m) une nouvelle solution

$$(\mathrm{K}_1 t_1 + \mathrm{K}_2 t_2 + \ldots + \mathrm{K}_m t_m),$$

dont les éléments sont

$$k_{1,r}t_1 + k_{2,r}t_2 + k_{3,r}t_3 + \ldots + k_{m,r}t_m \qquad (r = 1, 2, \ldots, n+1).$$

Nous dirons qu'un système de solutions (K_1), (K_2), $\ldots$, (K_m) forme un *système fondamental* de solutions, dans le cas où l'on obtient *toutes* les solutions de l'équation proposée, et chaque solution, *une seule fois*, en donnant à t_1, t_2, $\ldots$, t_m toutes les valeurs entières de $-\infty$ à $+\infty$ dans l'expression

$$(\mathrm{K}_1 t_1 + \mathrm{K}_2 t_2 + \ldots + \mathrm{K}_m t_m).$$

L'existence de ces systèmes fondamentaux ne fait pas de doute; nous avons obtenu déjà (théorème VII) un système fondamental composé de n solutions.

Théorème VIII. — *Un système fondamental de solutions se compose nécessairement de n solutions indépendantes.*

D'abord, les solutions qui composent un système fondamental $(\mathrm{K}_1, \mathrm{K}_2, \ldots, \mathrm{K}_m)$ sont nécessairement indépendantes. En effet, dans le cas contraire, on sait qu'il existe une relation identique

$$(\mathrm{K}_1 u_1 + \mathrm{K}_2 u_2 + \ldots + \mathrm{K}_m u_m) = 0.$$

les $u_1, u_2, \ldots, u_m$ n'étant pas tous nuls. On obtiendrait donc la solution

$$x_1 = x_2 = \ldots = x_{n+1} = 0,$$

non seulement en prenant

$$t_1 = t_2 = \ldots = t_m = 0,$$

mais encore en prenant

$$t_1 = u_1, \qquad t_2 = u_2, \qquad \ldots, \qquad t_m = u_m,$$

ce qui est contraire à la définition d'un système fondamental.

Et en second lieu, on a nécessairement $m = n$. En effet, la supposition de $m < n$ est inadmissible, car il en résulterait que $m+1$ solutions quelconques ne pourraient jamais être indépendantes. Or, le système fondamental que nous avons obtenu se compose effectivement de n solutions indépendantes, dont les déterminants (d'après le n° 21) sont $a_k : d$ ($k = 1, 2, \ldots, n+1$).

24. On s'assure facilement que n solutions indépendantes quelconques $(K_1), (K_2), \ldots, (K_n)$ ne forment pas toujours un système fondamental de solutions. Car si l'on cherche à représenter une solution quelconque par

$$(K_1 t_1 + K_2 t_2 + \ldots + K_n t_n),$$

on trouve bien toujours des valeurs déterminées pour $t_1, t_2, \ldots, t_n$, mais ces valeurs seront en général *fractionnaires*.

Théorème IX. — *Un système de n solutions indépendantes, tel que le plus grand commun diviseur de ses déterminants*

$$M_1, \quad M_2, \quad \ldots, \quad M_{n+1}$$

est $= 1$, *forme un système* fondamental *de solutions*.

En effet, si l'on cherche à représenter par

$$(K_1 t_1 + K_2 t_2 + \ldots + K_n t_n)$$

une solution quelconque $b_1, b_2, \ldots, b_{n+1}$, on obtient, pour déterminer $t_1, t_2, \ldots, t_n$, un système de $n+1$ équations linéaires, mais ces équations sont compatibles à cause de la relation

$$a_1 b_1 + a_2 b_2 + \ldots + a_{n+1} b_{n+1} = 0.$$

On peut donc, pour déterminer les inconnues, faire abstraction d'une quelconque de ces équations, et l'on obtient ainsi $n+1$ systèmes de n équations dont les déterminants sont $M_1, M_2, \ldots, M_{n+1}$. La valeur de t_k se présentera donc sous la

forme

$$t_k = \frac{p_1}{M_1} = \frac{p_2}{M_2} = \ldots = \frac{p_{n+1}}{M_{n+1}},$$

$p_1, p_2, \ldots, p_{n+1}$ étant des nombres entiers. Mais, si la valeur fractionnaire irréductible de t_k est $\frac{r}{s}$, s divisera $M_1, M_2, \ldots, M_{n+1}$. On a donc $s = 1$, c'est-à-dire t_k a une valeur *entière* et les solutions indépendantes $(K_1, K_2, \ldots, K_n)$ forment un système fondamental, ce qu'il fallait démontrer. Il est clair que les déterminants de n solutions indépendantes sont proportionnels à $a_1, a_2, \ldots, a_{n+1}$ (*voir* n° 21).

Théorème X. — *Les déterminants d'un système fondamental de solutions sont, abstraction faite des signes,*

$$a_1 : d, \quad a_2 : d, \quad \ldots, \quad a_{n+1} : d.$$

Désignons par $(\Lambda_1), (\Lambda_2), \ldots, (\Lambda_n)$ le système fondamental particulier que nous avons obtenu et dont les déterminants sont $a_k : d (k = 1, 2, \ldots, n+1)$. Alors $(K_1), (K_2), \ldots, (K_n)$ étant un autre système fondamental, on aura

$$\begin{aligned}
(\alpha_1 K_1 + \alpha_2 K_2 + \ldots + \alpha_n K_n) &= (\Lambda_1), \\
(\beta_1 K_1 + \beta_2 K_2 + \ldots + \beta_n K_n) &= (\Lambda_2), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\ldots, \\
(\lambda_1 K_1 + \lambda_2 K_2 + \ldots + \lambda_n K_n) &= (\Lambda_n).
\end{aligned}$$

On voit par là qu'un déterminant quelconque $a_k : d$, du système fondamental $(\Lambda_1), (\Lambda_2), \ldots, (\Lambda_n)$ est égal au déterminant correspondant du système fondamental $(K_1), (K_2), (K_n)$ multiplié par

$$\Delta = \begin{vmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \beta_1 & \beta_2 & \ldots & \beta_n \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_1 & \lambda_2 & \ldots & \lambda_n \end{vmatrix}.$$

On a donc nécessairement $\Delta \pm 1$.

La liaison des divers systèmes fondamentaux est évidente. On voit que chaque système fondamental fournit une solution du problème que nous avons considéré dans le n° 21.

25. La méthode la plus simple pour obtenir un système fondamental de solutions se fonde sur la remarque suivante.

Supposons que l'un des coefficients $a_1, a_2, \ldots, a_{n+1}$ soit égal à

$$d = (a_1, a_2, \ldots, a_{n+1}),$$

par exemple $a_{n+1} = d$. Alors il est clair que, pour avoir toutes les solutions de

l'équation indéterminée

$$a_1x_1 + a_2x_2 + \dots + a_nx_n + a_{n+1}x_{n+1} = 0,$$

il suffit de donner à $x_1, x_2, \dots, x_n$ des valeurs entières quelconques et à x_{n+1} la valeur (entière aussi) qui en est une conséquence. On a donc, dans ce cas, immédiatement un système fondamental de solutions correspondant à la solution générale

$$x_1 = t_1, \quad x_2 = t_2, \quad \dots, \quad x_n = t_n, \quad x_{n+1} = -\frac{a_1t_1 + a_2t_2 + \dots + a_nt_n}{d}.$$

Si le cas particulier que nous avons considéré ne se présente pas, soit a_1 le coefficient non nul, dont la valeur absolue est la plus petite. En posant

$$a_2 = k_1a_1 + b_2, \quad a_3 = k_2a_1 + b_3, \quad \dots, \quad a_{n+1} = k_na_1 + b_{n+1},$$
$$x'_1 = x_1 + k_1x_2 + k_2x_3 + \dots + k_nx_{n+1},$$

on aura une équation transformée

$$a_1x'_1 + b_2x_2 + b_3x_3 + \dots + b_{n+1}x_{n+1} = 0.$$

Par un choix convenable de $k_1, k_2, \dots, k_n$ on peut faire en sorte que le plus petit coefficient de l'équation transformée soit moindre que a_1 ou même ne surpasse pas $\frac{1}{2}a_1$. En continuant ainsi, on tombe finalement sur une équation dont un des coefficients est d et dont on peut écrire immédiatement un système fondamental de solutions auquel correspondra un système fondamental de solutions de l'équation proposée. Cette méthode, qui s'applique également à l'équation

$$a_1x_1 + a_2x_2 + \dots + a_{n+1}x_{n+1} = u,$$

se trouve dans un Mémoire posthume d'Euler. Jacobi l'a rappelée à l'attention des géomètres dans un Mémoire également posthume (*Journal de Crelle*, t. 69, p. 21).

26. Les nombres $a, b, c, \dots, l$ étant premiers entre eux et

$$m = abc \dots l,$$

nous savons que le plus grand commun diviseur des nombres $\frac{m}{a}, \frac{m}{b}, \dots, \frac{m}{l}$ est $= 1$. N étant un nombre quelconque, on pourra donc toujours satisfaire à l'équation

$$N = a_1\frac{m}{a} + b_1\frac{m}{b} + \dots + l_1\frac{m}{l},$$

c'est-à-dire on aura

$$\frac{N}{abc\ldots l} = \frac{a_1}{a} + \frac{b_1}{b} + \ldots + \frac{l_1}{l}.$$

On verra facilement que la fraction $\frac{N}{abc\ldots l}$ peut se mettre d'une seule manière sous la forme

$$E + \frac{a_2}{a} + \frac{b_2}{b} + \ldots + \frac{l_2}{l},$$

E étant un entier positif ou négatif et

$$0 \leq a_2 < a, \qquad 0 \leq b_2 < b, \qquad 0 \leq l_2 < l.$$

La solution de l'équation indéterminée $ax - My = 1$ a été donnée en Europe, pour la première fois, par Bachet de Méziriac (*Problèmes plaisants et délectables, qui se font par les nombres*. 2e édition; 1624. 5e édition, par Labosne; 1884). Les anciens géomètres hindous, Bhaseara et Brahmegupta connaissaient aussi déjà la solution de ce problème.

Le problème du n° 11 se trouve traité complètement dans d'anciens Livres d'Arithmétique chinois. On y trouve non seulement la méthode de Gauss (n° 13), mais aussi la réduction du cas général au cas où les modules sont premiers entre eux (n° 15). On peut voir sur cette question

BIERNATZKI, *Journal de Crelle*, t. 52.
J. BERTRAND, *Journal des Savants*, 1869.
MATTHIESSEN, *Journal de Crelle*, t. 91.

La fonction $\varphi(M)$ a été considérée pour la première fois par Euler. Les Mémoires d'Euler sur l'Arithmétique ont été réunis en deux volumes (*Leonhardi Euleri Commentationes arithmeticæ collectæ*. Petropoli, 1849). Nous citerons toujours cette édition; la fonction φ se rencontre dans le Mémoire *Theoremata arithmetica nova methodo demonstrata*, 1759 (tome I, p. 274). La démonstration d'Euler est reproduite dans le tome II de l'*Algèbre* de Serret. Le théorème $\Sigma\varphi(d) = M$ est dû à Gauss (*Disquisitiones arithmeticæ*, 1801, art. 39; tome I des *Œuvres complètes*).

Les théorèmes de Lagrange sur les congruences se trouvent dans le Mémoire : *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers* (*Œuvres*, t. II) et la démonstration des théorèmes de Fermat et de Wilson. *Œuvres*, t. III, p. 425.

La considération d'un système fondamental de solutions d'une ou de plusieurs équations indéterminées est due à M. H.-J. Stephen Smyth (*Philosophical Transactions of the Royal Society for the year* 1861; vol. 151).

Nous indiquerons ici les principaux Ouvrages d'un caractère général sur la théorie des nombres :

Gauss. *Disquisitiones arithmeticæ* (*Œuvres*, t. I). Il y a une traduction française par Poullet-Delisle.

Legendre. *Théorie des nombres*, 3e édition.

Smyth. *Report on the theory of Numbers* (*British Association for the advancement of Science*, 1859, 1860, 1861, 1862, 1863, 1865).

C'est là un résumé extrêmement important sur toutes les parties de la théorie des nombres auquel nous aurons à emprunter beaucoup de choses.

Lejeune-Dirichlet, *Vorlesungen über Zahlentheorie*, herausgegeben von R. Dedekind. Dritte Auflage, 1879.

Serret, *Traité d'Algèbre*, 5e édition, t. II.

CHAPITRE III.

ÉQUATIONS LINÉAIRES INDÉTERMINÉES, SYSTÈMES DE CONGRUENCES LINÉAIRES.

1. Considérons le système des congruences

$$a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n \equiv u_i \pmod{M}.$$

Soit $\Delta = |a_{ik}|$ le déterminant formé avec les coefficients des inconnues, puis α_{ik} le coefficient de a_{ik} dans Δ. On obtient immédiatement

$$\Delta x_i \equiv u_1\alpha_{1i} + u_2\alpha_{2i} + \ldots + u_n\alpha_{ni} \pmod{M}.$$

Supposons que Δ soit premier avec le module M, alors cette dernière relation détermine une valeur unique de x_i par rapport au module M; et ensuite il est facile de voir que les valeurs de $x_1, x_2, \ldots, x_n$ ainsi obtenues satisfont bien aux conditions proposées. En effet, on trouve

$$\Delta(a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n) \equiv \Delta u_i \pmod{M}$$

et, puisque Δ est premier avec M, on peut diviser par Δ.

Le système des congruences admet donc une solution unique dans le cas particulier que nous considérons. On peut ajouter que les valeurs de $x_1, x_2, \ldots, x_n$ satisferont encore à la relation

$$a_{n+1,1}x_1 + a_{n+1,2}x_2 + \ldots + a_{n+1,n}x_n \equiv u_{n+1} \pmod{M}$$

si l'on a

$$\begin{vmatrix} a_{1,1} & a_{1n} & u_1 \\ \cdots & \cdots & \cdots \\ a_{n1} & a_{nn} & u_n \\ a_{n+1,1} & a_{n+1,n} & u_{n+1} \end{vmatrix} \equiv 0 \pmod{M}.$$

En effet, il est facile de voir que cette dernière congruence peut s'écrire sous cette forme

$$\Delta(u_{n+1} - a_{n+1,1}x_1 - a_{n+1,2}x_2 - \ldots - a_{n+1\,n}x_n) \equiv 0 \pmod{M}.$$

2. Les résultats précédents sont ceux qui s'offrent immédiatement lorsqu'on poursuit l'analogie évidente qui existe entre la théorie des congruences et la

théorie des équations. Mais si Δ n'est pas premier avec M, une étude plus approfondie est nécessaire. Elle a été faite pour la première fois par M. H.-J.-S. Smith, et nous allons exposer sa théorie. Les considérations suivantes interviennent non seulement dans des questions de la théorie des nombres, mais elles sont encore utiles dans beaucoup de théories d'analyse pure; aussi plusieurs résultats isolés ont été obtenus antérieurement par d'autres géomètres.

Nous commencerons par étudier les équations linéaires indéterminées, mais il convient d'abord de fixer le sens de quelques expressions dont nous ferons usage.

En adoptant une expression introduite, croyons-nous, par M. Sylvester, nous appellerons *matrice* un Tableau de forme rectangulaire

$$\begin{matrix} a_{1,1} & a_{1,2} & \dots & a_{1m}, \\ a_{2,1} & a_{2,2} & \dots & a_{2m}, \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,m} \end{matrix}$$

contenant mn quantités données, et nous dirons que cette matrice est du type $n \times m$. Si l'on a un système quelconque d'équations linéaires, les coefficients des inconnues constituent la matrice de ce système. Si les équations ne sont pas homogènes, on peut ajouter à cette matrice une dernière colonne formée par les termes connus. On obtient ainsi la *matrice complétée* du système. Les mêmes expressions s'emploieront dans le cas d'un système de congruences. Les éléments a_{ik} seront toujours des nombres entiers.

Les déterminants d'une matrice sont les déterminants de degré le plus élevé que l'on peut former avec les lignes ou les colonnes de la matrice; ainsi, dans le cas $m > n$, ces déterminants renferment n^2 éléments et leur nombre est

$$\frac{m(m-1)\dots(m-n+1)}{1.2\dots n} = (m)_n.$$

Le plus grand diviseur d'une matrice est le plus grand commun diviseur des déterminants de cette matrice, en supposant que ces déterminants ne soient pas tous nuls. Dans le cas $m = n$, ce plus grand diviseur est le déterminant même du système des n^2 éléments.

Nous désignerons une matrice souvent par le symbole

$$\| A \|$$

et, dans le cas où elle est du type $n \times n$, $| A |$ sera le déterminant. Deux matrices

$$\| A \| \quad \text{et} \quad \| B \|$$

des types $m \times (m+n)$ et $n \times (m+n)$ sont de types *complémentaires*. Il est

clair que ces matrices ont le même nombre de déterminants, et l'on peut faire correspondre à chaque déterminant de $\| A \|$ un déterminant de $\| B \|$ et réciproquement, de la manière suivante.

En écrivant la matrice $\| B \|$ en dessous de la matrice $\| A \|$ on obtient une matrice

$$\left\| \begin{matrix} A \\ B \end{matrix} \right\|$$

qui sera du type $(m+n) \times (m+n)$ et à un déterminant de $\| A \|$ on fera correspondre le déterminant de $\| B \|$ avec lequel il se trouve multiplié dans le déterminant des $(m+n)^2$ éléments

$$\left| \begin{matrix} A \\ B \end{matrix} \right|.$$

Souvent il n'y a pas d'intérêt à faire attention au signe d'un déterminant d'une matrice, mais dans le cas actuel il convient de faire en sorte que le produit des déterminants correspondants se retrouve avec son signe dans le déterminant des $(m+n)^2$ éléments.

3. Les déterminants d'une matrice ne sont pas indépendants; il existe en général un grand nombre de relations identiques entre eux. Nous allons nous rendre compte d'abord de la nature de ces relations et du nombre des déterminants qui sont indépendants. On pourra considérer dans ce numéro les éléments de la matrice comme des quantités arbitraires. Considérons la matrice

$$(1) \qquad \left\| \begin{matrix} a_{1,1} & a_{1,2} & \ldots & a_{1,m+n}, \\ a_{2,1} & a_{2,2} & \ldots & a_{2,m+n}, \\ \ldots & \ldots & \ldots & \ldots\ldots\ldots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,m+n} \end{matrix} \right\|$$

du type $m \times (m+n)$. Le nombre des déterminants est

$$\frac{(n+1)(n+2)\ldots(n+m)}{1.2.3\ldots m},$$

mais nous allons montrer qu'il y en a seulement $mn+1$ qui sont indépendants. Tous les déterminants peuvent s'exprimer à l'aide de $mn+1$ d'entre eux.

Soit

$$(2) \qquad \Delta = | a_{ik} | \qquad (i, k = 1, 2, \ldots, m)$$

le déterminant formé par les m premières colonnes de la matrice. Le déterminant obtenu en remplaçant dans Δ la $i^{\text{ème}}$ colonne par la $m+k^{\text{ième}}$ colonne de la matrice sera désigné par $\Delta_{i,m+k}$. On déduit ainsi de Δ mn nouveaux déterminants, i

variant de 1 à m, k de 1 à n. On pourra les disposer dans le Tableau

$$(3)\qquad \left\{\begin{array}{llll} \Delta_{1,m+1} & \Delta_{2,m+2} & \ldots & \Delta_{1,m+n}, \\ \Delta_{2,m+1} & \Delta_{2,m+2} & \ldots & \Delta_{2,m+n}, \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \Delta_{m,m+1} & \Delta_{m,m+2} & \ldots & \Delta_{m,m+n}. \end{array}\right.$$

Les $mn+1$ déterminants Δ, $\Delta_{i,m+k}$ sont indépendants; on peut trouver une matrice pour laquelle ces déterminants ont des valeurs données d'avance. Prenons d'abord arbitrairement les éléments a_{ik} de Δ, avec la seule restriction de vérifier la relation (2). On a ainsi les m premières colonnes de la matrice. On peut déterminer ensuite la $m+k^{\text{ième}}$ colonne par la condition que les déterminants $\Delta_{i,m+k}\,(i=1, 2, \ldots, m)$ prennent des valeurs données. En effet, on obtient ainsi m équations linéaires pour déterminer

$$a_{1,m+k},\quad a_{2,m+k},\quad \ldots,\quad a_{m,m+k}.$$

Le déterminant de ce système est Δ^{m-1}, mais, en le résolvant, on trouve simplement

$$(4)\qquad \begin{gathered} a_{i,m+k} = (a_{i,1}\Delta_{1,m+k} + a_{i,2}\Delta_{2,m+k} + \ldots + a_{im}\Delta_{m,m+k}) : \Delta, \\ i = 1, 2, 3, \ldots, m, \\ k = 1, 2, 3, \ldots, n. \end{gathered}$$

La vérification de ces valeurs est du reste immédiate, et l'indépendance des $mn+1$ déterminants Δ, $\Delta_{i,m+k}$ est manifeste.

Considérons maintenant un autre déterminant Δ' de la matrice. Il contiendra k colonnes appartenant aux n dernières colonnes de la matrice ($k \geqq 2$); soient

$$m+\lambda_1,\qquad m+\lambda_2,\qquad \ldots,\qquad m+\lambda_k$$

les rangs de ces colonnes. Les autres $m-k$ colonnes de Δ' appartiendront aux m premières colonnes de la matrice, c'est-à-dire, ce sont des colonnes de Δ. Soient

$$\mu_1,\quad \mu_2,\quad \ldots,\quad \mu_k$$

les rangs des colonnes de Δ qui ne figurent pas dans Δ'. En remplaçant alors dans Δ' les éléments $a_{i,m+k}$ par leurs valeurs (4), on obtient, à l'aide des propriétés élémentaires des déterminants, la formule

$$(5)\qquad \Delta' = \pm \begin{vmatrix} \Delta_{\mu_1,m+\lambda_1} & \Delta_{\mu_1,m+\lambda_2} & \ldots & \Delta_{\mu_1,m+\lambda_k} \\ \Delta_{\mu_2,m+\lambda_1} & \Delta_{\mu_2,m+\lambda_2} & \ldots & \Delta_{\mu_2,m+\lambda_k} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \Delta_{\mu_k,m+\lambda_1} & \Delta_{\mu_k,m+\lambda_2} & \ldots & \Delta_{\mu_k,m+\lambda_k} \end{vmatrix} : \Delta^{k-1}.$$

Ainsi tous les déterminants de la matrice s'expriment rationnellement au moyen des $mn+1$ déterminants Δ, $\Delta_{i,m+k}$. On voit que Δ' est égal à un déterminant mineur du degré k, puisé dans la matrice (3), divisé par Δ^{k-1}. Le nombre des déterminants tels que Δ' est

$$(m)_2(n)_2+(m)_3(n)_3+(m)_4(n)_4+\ldots$$
$$=(m+n)_m-(m)_0(n)_0-(m)_1(n)_1=(m+n)_m-(mn+1).$$

Équations linéaires indéterminées.

4. Considérons d'abord le système linéaire et homogène

$$(1)\qquad \begin{cases} a_{i,1}x_1+a_{i,2}x_2+\ldots+a_{i,m+n}x_{m+n}=0, \\ i=1,2,\ldots,m. \end{cases}$$

Nous supposerons que ces équations sont linéairement indépendantes, c'est-à-dire que tous les déterminants de la matrice de ce système ne sont pas nuls. Le plus grand diviseur de la matrice a alors une signification précise, soit d ce plus grand diviseur.

Le moyen que nous emploierons pour trouver toutes les solutions en nombres entiers consiste dans l'introduction de nouvelles inconnues.

Au lieu de $x_1, \ldots, x_{m+n}$, on peut introduire de nouvelles inconnues, en posant

$$x_i=c_{i,1}x'_1+c_{i,2}x'_2+\ldots+c_{i,m+n}x'_{m+n},$$
$$i=1,2,\ldots,m+n.$$

Les $c_{i,k}$ seront des nombres entiers, et nous n'emploierons que des substitutions dont le déterminant $|c_{i,k}|=\pm 1$.

On peut alors exprimer réciproquement les x'_i par des fonctions linéaires à coefficients entiers des x_i, et, comme nous ne considérons que les solutions en nombres entiers, le système transformé sera absolument équivalent au système donné, c'est-à-dire à deux solutions distinctes d'un des systèmes correspondront toujours deux solutions également distinctes de l'autre.

Parmi les déterminants de la matrice de (1) qui ne sont pas nuls, il y en aura au moins un dont la valeur absolue est le plus petit. Nous pouvons supposer, en adoptant la notation du n° 3, que Δ soit ce déterminant *minimum*. Supposons d'abord que tous les déterminants $\Delta_{i,m+k}$ soient divisibles par Δ. Alors il est clair que l'on obtient la solution la plus générale de (1) en donnant à $x_{m+1}, x_{m+2}, \ldots, x_{m+n}$ des valeurs entières absolument quelconques et en déterminant ensuite

$x_1, \ldots, x_m$ par les formules

$$x_i = -(\Delta_{i,m+1} x_{m+1} + \Delta_{i,m+2} x_{m+2} + \ldots + \Delta_{i,m+n} x_{m+n}) : \Delta.$$
$$(i = 1, 2, \ldots m).$$

On voit, du reste, par la formule (5) du n° 3, que, lorsque Δ divise tous les $\Delta_{i,m+k}$, il divisera tous les déterminants de la matrice, en sorte que l'on doit avoir $\Delta = \pm d$.

Mais supposons que Δ ne divise pas tous les $\Delta_{i,m+k}$ et, par exemple, ne divise pas $\Delta_{1,m+1}$. Alors, on peut toujours trouver un entier c tel que la valeur absolue de

$$\Delta_{1,m+1} - c\Delta$$

soit inférieure à celle de Δ. La substitution de déterminant $+1$

$$x_i = x'_i \qquad (i = 1, 2, 3, \ldots, m, m+2, m+3, \ldots, m+n),$$
$$x_{m+1} = x'_{m+1} - c x'_1$$

transformera alors le système (I) dans un autre système dans lequel un des déterminants est $\Delta_{1,m+1} - c\Delta$. Le déterminant minimum du système transformé est donc plus petit (en valeur absolue) que Δ. Si ce déterminant minimum ne divise pas tous les autres déterminants, on pourra encore le diminuer par le même procédé. Il est clair que l'on finira par trouver un système transformé dans lequel le déterminant minimum divise tous les autres déterminants, et dont on peut écrire alors immédiatement la solution la plus générale. Cette solution renferme, comme nous l'avons vu, n indéterminées auxquelles on peut donner toutes les valeurs entières de $-\infty$ à $+\infty$.

Théorème I. — *On obtient toutes les solutions du système* (I), *et chaque solution une seule fois, par les formules*

$$\text{(II)} \qquad \begin{cases} x_i = \beta_{1,i} t_1 + \beta_{2,i} t_2 + \ldots + \beta_{n,i} t_n, \\ (i = 1, 2, \ldots, m+n), \end{cases}$$

en donnant à $t_1, t_2, \ldots, t_n$ toutes les valeurs entières de $-\infty$ à $+\infty$.

Il est clair qu'en substituant les expressions (II) dans le système (I), les coefficients de $t_1, t_2, \ldots, t_n$ doivent s'annuler.

On obtiendrait donc encore des solutions de (I) en donnant à $t_1, \ldots, t_n$ des valeurs fractionnaires. Mais il est clair que l'on ne peut jamais obtenir, de cette façon, une solution de (I) en nombres entiers, car *toute* solution entière correspond à un système unique de valeurs entières de $t_1, \ldots, t_n$.

Pour obtenir, dans un cas donné, la solution générale sous la forme (II), il sera plus pratique de procéder autrement. On cherchera, par exemple, par la méthode d'Euler (Chap. II, 25), la solution générale de

$$a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,m+n}x_{m+n} = 0,$$

qui renfermera $m+n-1$ indéterminées, puis on introduira ces valeurs dans la seconde équation

$$a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,m+n}x_{m+n} = 0,$$

etc., jusqu'à ce que l'on ait épuisé les m relations données.

Si l'on transforme, comme nous l'avons fait, le système (I), il est clair que tout déterminant du système transformé est une fonction linéaire à coefficients entiers des déterminants de (I), et réciproquement. On voit par là que le plus grand diviseur des deux matrices est le même et, par conséquent, dans le procédé que nous avons employé plus haut, on trouvera finalement un système dont la matrice a un déterminant minimum égal à $\pm d$.

5. Considérons r solutions du système (I)

$$\begin{array}{llll} \alpha_{1,1}, & \alpha_{1,2}, & \ldots, & \alpha_{1,m+n}, \\ \alpha_{2,1}, & \alpha_{2,2}, & \ldots, & \alpha_{2,m+n}, \\ \ldots, & \ldots, & \ldots, & \ldots\ldots, \\ \alpha_{r,1}, & \alpha_{r,2}, & \ldots, & \alpha_{r,m+n}, \end{array}$$

que nous désignerons quelquefois aussi par de simples lettres $A_1, A_2, \ldots, A_r$. Ces solutions sont *indépendantes* si tous les déterminants de degrés r ne sont pas nuls. Il est clair que l'on peut trouver tout au plus n solutions indépendantes, car, puisque toutes les solutions sont comprises dans les formules (II) (n° 4) qui ne renferment que n indéterminées, $n+1$ solutions ne sont jamais indépendantes. En multipliant les solutions précédentes par $t_1, t_2, \ldots, t_r$ et en ajoutant, on obtient une nouvelle solution

$$A_1t_1 + A_2t_2 + \ldots + A_rt_r$$

dont les éléments sont

$$x_i = \alpha_{1,i}t_1 + \alpha_{2,i}t_2 + \ldots + \alpha_{r,i}t_r.$$

Nous dirons que les solutions

$$A_1, \quad A_2, \quad \ldots, \quad A_r$$

forment un *système fondamental de solutions*, lorsque l'on obtient toutes les solutions possibles, et chaque solution une seule fois, en donnant à $t_1, t_2, \ldots, t_r$

les valeurs entières de $-\infty$ à $+\infty$. L'existence de ces systèmes fondamentaux de solutions ne fait pas de doute, car nous savons, par le théorème I, que

$$\beta_{i,1},\quad \beta_{i,2},\quad \ldots,\quad \beta_{i,m+n}$$
$$(i = 1, 2, \ldots, n)$$

est un tel système.

Théorème II. — *Un système fondamental de solutions se compose de n solutions indépendantes.*

Ce théorème est une généralisation du théorème VIII du Chapitre II; la démonstration est exactement la même.

La matrice formée par n solutions indépendantes, ou par un système fondamental de solutions, est du type $n \times (m+n)$, donc du type complémentaire de la matrice du système (I).

Considérons la matrice du système (I) et la matrice formée par n solutions indépendantes

$$\begin{array}{cccc} a_{1,1}, & a_{1,2}, & \ldots, & a_{1,m+n}, \\ \ldots, & \ldots, & \ldots, & \ldots\ldots, \\ a_{m,1}, & a_{m,2}, & \ldots, & a_{m,m+n}, \end{array}$$

$$\begin{array}{cccc} \alpha_{1,1}, & \alpha_{1,2}, & \ldots, & \alpha_{1,m+n}, \\ \ldots, & \ldots, & \ldots, & \ldots\ldots, \\ \alpha_{n,1}, & \alpha_{n,2}, & \ldots, & \alpha_{n,m+n}. \end{array}$$

Les relations qui existent entre ces nombres se réduisent à ceci : que la somme obtenue en multipliant les éléments d'une quelconque des m premières lignes par les éléments correspondants d'une des n dernières lignes est nulle.

On voit donc qu'il y a une réciprocité complète entre les deux matrices, et si l'on considère le système indéterminé

$$\alpha_{i,1}x_1 + \alpha_{i,2}x_2 + \ldots + \alpha_{i,m+n}x_{m+n} = 0$$
$$(i = 1, 2, \ldots, n),$$

les nombres

$$a_{i,1},\quad a_{i,2},\quad \ldots,\quad a_{i,m+n}$$
$$(i = 1, 2, \ldots, m),$$

en donneront m solutions indépendantes.

D'après ce que nous avons dit dans le n° 2, on peut faire correspondre à chaque déterminant de la matrice $\|a_{i,k}\|$ un déterminant de la matrice $\|\alpha_{i,k}\|$ d'un système de n solutions indépendantes.

Théorème III. — *La matrice d'un système fondamental de solutions a l'unité pour plus grand diviseur.*

Considérons, en effet, les formules

$$x_i = \beta_{1,i}t_1 + \beta_{2,i}t_2 + \ldots + \beta_{n,i}t_n,$$
$$[i = 1, 2, \ldots, (m + n)]$$

qui renferment la solution la plus générale. Il est clair d'abord que

$$(\beta_{1,1}\beta_{1,2}\ldots\beta_{1,m+n}) = 1,$$

car, si ces nombres étaient tous divisibles par $c > 1$, on trouverait une solution entière en posant $t_1 = \frac{1}{c}$, ce qui, on le voit facilement d'après ce que nous avons dit plus haut, est contraire à la nature d'un système fondamental de solutions.

Ensuite, je dis que les déterminants de la matrice

$$\begin{matrix} \beta_{1,1}, & \beta_{1,2}, & \ldots, & \beta_{1,m+n}, \\ \beta_{2,1}, & \beta_{2,2}, & \ldots, & \beta_{2,m+n} \end{matrix}$$

ont aussi 1 pour plus grand commun diviseur. Car si ces déterminants étaient tous divisibles par $c > 1$, c ne divisera pas tous les éléments de la première ligne, par exemple c ne divisera pas $\beta_{1,1}$; mais alors on trouverait encore une solution entière en posant

$$t_1 = -\frac{\beta_{2,1}}{c}, \qquad t_2 = +\frac{\beta_{1,1}}{c},$$

ce qui est impossible.

Ensuite, je dis que le plus grand commun diviseur de la matrice

$$\begin{matrix} \beta_{1,1}, & \beta_{1,2}, & \ldots, & \beta_{1,m+n}, \\ \beta_{2,1}, & \beta_{2,2}, & \ldots, & \beta_{2,m+n}, \\ \beta_{3,1}, & \beta_{3,2}, & \ldots, & \beta_{3,m+n} \end{matrix}$$

est encore $= 1$. Car si ce plus grand diviseur était $c > 1$, c ne diviserait pas, par exemple, le déterminant

$$\begin{vmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{vmatrix},$$

et, en posant

$$t_1 = \begin{vmatrix} \beta_{2,1} & \beta_{2,2} \\ \beta_{3,1} & \beta_{3,2} \end{vmatrix} : c, \qquad t_2 = \begin{vmatrix} \beta_{3,1} & \beta_{3,2} \\ \beta_{1,1} & \beta_{1,2} \end{vmatrix} : c, \qquad t_3 = \begin{vmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{vmatrix} : c,$$

on trouverait encore une solution entière, ce qui est impossible.

Il est clair que l'on peut continuer ainsi, pour arriver au théorème énoncé.

6. En cherchant à exprimer une solution quelconque

$$\alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_{m+n}$$

par un système fondamental de solution $\beta_{i,k}$, on est amené à déterminer n inconnues $t_1, t_2, \ldots, t_n$ par $m+n$ équations

$$\alpha_i = \beta_{1,i}t_1 + \beta_{2,i}t_2 + \ldots + \beta_{n,i}t_n$$
$$(i = 1, 2, \ldots, m+n).$$

On sait d'avance qu'il existe une solution unique et en nombres entiers; ce système linéaire doit donc présenter certaines circonstances particulières. Nous allons montrer qu'elles se réduisent à ceci : d'abord le plus grand diviseur de la matrice du système est $= 1$, ensuite tout déterminant de la matrice complétée est nul, car cette matrice complétée se compose de $n+1$ solutions.

Théorème IV. — *Un système de $m+n$ équations entre n inconnues*

$$\alpha_i = \beta_{1,i}t_1 + \beta_{2,i}t_2 + \ldots + \beta_{n,i}t_n$$
$$(i = 1, 2, \ldots, m+n)$$

admet toujours une solution unique et en nombres entiers, lorsque le plus grand diviseur de la matrice du système est $= 1$ et que tous les déterminants de la matrice complétée sont nuls.

Nous ajouterons un théorème analogue sur les congruences.

Théorème V. — *Un système de $m+n$ congruences entre n inconnues*

$$\alpha_i \equiv \beta_{1,i}t_1 + \beta_{2,i}t_2 + \ldots + \beta_{n,i}t_n \pmod{M},$$
$$(i = 1, 2, \ldots, m+n)$$

admet toujours une solution unique, lorsque le plus grand diviseur de la matrice du système est premier avec M et que tous les déterminants de la matrice complétée sont $\equiv 0 \pmod{M}$.

Il suffira de démontrer ce dernier théorème; nous pouvons écrire les congruences données ainsi

$$A_i \equiv \alpha_i \pmod{M}, \qquad (i = 1, 2, \ldots, m+n),$$

les A_i étant des fonctions linéaires en $t_1, \ldots, t_n$. Considérons le déterminant minimum Δ de la matrice de ce système. Si Δ divise tous les autres déterminants, il sera premier avec M d'après notre hypothèse. Les n congruences correspondantes admettront alors une solution unique et cette solution satisfera aussi à toutes les autres congruences (*voir* le n° 1).

Mais si

$$\Delta = |\beta_{i,k}| \qquad (i, k = 1, 2, \ldots, n)$$

ne divise pas tous les autres déterminants, il ne divisera pas, par exemple, le déterminant

$$\begin{vmatrix} \beta_{1,n+1} & \beta_{2,n+1} & \ldots & \beta_{n,n+1} \\ \beta_{1,2} & \beta_{2,2} & \ldots & \beta_{n,2} \\ \beta_{1,3} & \beta_{2,3} & \ldots & \beta_{n,3} \\ \ldots & \ldots & \ldots & \ldots \\ \beta_{1,n} & \beta_{2,n} & \ldots & \beta_{n,n} \end{vmatrix}.$$

Mais alors on pourra remplacer le système donné par le système équivalent

$$A_i = \alpha_i \qquad (i = 1, 2, \ldots, n, n+2, n+3, \ldots, n+m),$$
$$A_{n+1} - cA_1 = \alpha_{n+1} - c\alpha_1,$$

et ce nouveau système aura, pour une valeur convenable de c, un déterminant minimum plus petit que Δ. On pourra ainsi diminuer le déterminant minimum jusqu'à ce qu'il soit devenu égal au plus grand diviseur de la matrice donnée. Il divisera alors tous les autres déterminants et l'on est ramené au cas que nous avons considéré d'abord.

Le théorème IV peut se démontrer d'une façon toute semblable, ou encore par le raisonnement que nous avons fait dans la démonstration du théorème IX (Chapitre II).

Nous indiquerons encore une autre démonstration du théorème V.

Si l'on écrit

$$M = P \times Q \times R \times \ldots,$$

où P, Q, R, ... sont des puissances de nombres premiers distincts, on reconnaît facilement que les congruences données admettent une solution unique, par rapport à chacun des modules P, Q, R, ..., d'où l'on peut conclure qu'elles en admettent aussi une par rapport au module M.

7. *Multiplication des matrices.* — Soit

$$\| a_{i,k} \| \qquad \begin{pmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, m+n \end{pmatrix},$$

ou $\|A\|$ une matrice du type $n \times (m+n)$, $(m \geqq 0)$,

$$\| c_{i,k} \| \quad (i, k = 1, 2, \ldots, n),$$

ou $\|C\|$, une matrice du type $n \times n$, nous représenterons par

$$\|C\| \times \|A\| = \|A'\|$$

une matrice du même type que $\| A \|$ et dont les éléments sont

$$a'_{i,k} = c_{i,1}a_{1,k} + c_{i,2}a_{2,k} + \ldots + c_{i,n}a_{n,k}$$
$$\begin{pmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, m+n \end{pmatrix}.$$

Lorsque $\| C_1 \|$ est encore du type $n \times n$, nous écrirons

$$\| C_1 \| \times \| A' \| = \| C_1 \| \times \| C \| \times \| A \|.$$

et il est facile de voir que

$$\| C_1 \| \times \| C \| \times \| A \| = \| \, \| C_1 \| \times \| C \| \, \| \times \| A \|.$$

Mais on ne peut pas permuter les deux matrices dans un produit, et si l'on considère un produit de plusieurs facteurs

$$\| C_n \| \times \| C_{n-1} \| \times \ldots \times \| C \| \times \| A \|,$$

on suppose toujours que toutes les matrices $\| C_k \|$ sont du type $n \times n$: seule la matrice $\| A \|$ peut être du type $n \times (m+n)$, le produit est toujours du même type que $\| A \|$.

Il est clair que, lorsque

$$\| A' \| = \| C \| \times \| A \|,$$

tout déterminant de $\| A' \|$ est égal au déterminant correspondant de $\| A \|$ multiplié par le déterminant $| C |$. Les déterminants correspondants de $\| A \|$ et $\| A' \|$ seront proportionnels et si, en particulier, le plus grand diviseur de $\| A \|$ est $= 1$, le plus grand diviseur de $\| A' \|$ sera la valeur absolue de $| C |$.

Dans le cas où le déterminant

$$\begin{vmatrix} c_{1,1} & c_{1,2} & \ldots & c_{1,n} \\ c_{2,1} & c_{2,2} & \ldots & c_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n,1} & c_{n,2} & \ldots & c_{n,n} \end{vmatrix} = \varepsilon = \pm 1,$$

nous désignerons par $\| C \|^{-1}$ la matrice

$$\begin{matrix} \varepsilon\gamma_{1,1}, & \varepsilon\gamma_{2,1}, & \ldots, & \varepsilon\gamma_{n,1}, \\ \varepsilon\gamma_{1,2}, & \varepsilon\gamma_{2,2}, & \ldots, & \varepsilon\gamma_{n,2}, \\ \ldots, & \ldots, & \ldots, & \ldots, \\ \varepsilon\gamma_{1,n}, & \varepsilon\gamma_{2,n}, & \ldots, & \varepsilon\gamma_{n,n}, \end{matrix}$$

$\gamma_{i,k}$ étant le coefficient de $c_{i,k}$ dans le déterminant $| C |$.

On voit que

$$\|C\| \times \|C\|^{-1} = \|C\|^{-1} \times \|C\| = \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & . & \dots & . \\ 0 & . & \dots & 1 \end{vmatrix},$$

et de la relation

$$\|A'\| = \|C\| \times \|A\|,$$

on peut conclure

$$\|A\| = \|C\|^{-1} \times \|A'\|.$$

8. Soit $\|A\|$ la matrice formée par n solutions indépendantes, $\|B\|$ la matrice formée par un système fondamental de solutions.

Puisque les solutions de $\|A\|$ peuvent se déduire du système fondamental $\|B\|$, cela revient, avec notre nouvelle notation, à dire que

$$\|A\| = \|C\| \times \|B\|.$$

Il est clair que le plus grand diviseur de $\|A\|$ est $= \pm |C|$, et, dans le cas $|C| = \pm 1$, $\|A\|$ est évidemment aussi un système fondamental de solutions, car

$$\|B\| = \|C\|^{-1} \times \|A\|.$$

Si l'on considère plusieurs systèmes de n solutions indépendantes, ou de systèmes fondamentaux, les déterminants correspondants seront toujours proportionnels.

THÉORÈME VI. — *Lorsque le plus grand diviseur de la matrice*

$$\|B\| \quad \text{du type } n \times (m+n)$$

est $= 1$, *et que les déterminants d'une matrice*

$$\|A\| \quad \text{du type } n \times (m+n)$$

sont proportionnels aux déterminants correspondants de $\|B\|$, *on a toujours*

$$\|A\| = \|C\| \times \|B\|$$

et la matrice $\|C\|$ *est unique.*

En effet, on obtient pour déterminer $c_{i,1}, c_{i,2}, \dots, c_{i,n}$ les équations

$$a_{i,k} = c_{i,1} b_{1,k} + c_{i,2} b_{2,k} + \dots + c_{i,n} b_{n,k},$$
$$k = 1, 2, \dots, (m+n).$$

Un déterminant quelconque de la matrice complétée de ce système, tel que

$$\begin{vmatrix} b_{1,1} & b_{2,1} & b_{n,1} & a_{i,1} \\ b_{1,2} & b_{2,2} & b_{n,2} & a_{i,2} \\ \dots & \dots & \dots & \dots \\ b_{1,n+1} & b_{2,n+1} & b_{n,n+1} & a_{i,n+1} \end{vmatrix}$$

est nul, car d'après la proportionnalité supposée entre les déterminants de $\| A \|$ et de $\| B \|$, il est permis de remplacer partout $b_{i,k}$ par $a_{i,k}$, à condition de diviser après par un certain nombre entier le facteur de proportionnalité.

Mais on obtient ainsi un déterminant avec deux colonnes identiques. Donc, d'après le théorème IV, il existe un système et un seul de valeurs $c_{i,1}, c_{i,2}, \dots, c_{i,n}$ qui satisfont à la question.

On voit qu'une matrice du type $n \times (m+n)$ dont les déterminants (non tous nuls) sont proportionnels aux déterminants de la matrice $\| B \|$ formée avec un système fondamental (ou avec n solutions indépendantes) est nécessairement composée avec n solutions indépendantes.

Théorème VII. — *Les déterminants d'une matrice formée par n solutions indépendantes, du type $n \times (m+n)$, sont proportionnels aux déterminants correspondants de la matrice du type $m \times (m+n)$ du système indéterminé donné* (I). *En particulier, un déterminant d'un système fondamental de solutions est égal au déterminant correspondant du système* (I), *divisé par d.*

Il suffira de faire voir que le théorème se trouve vérifié pour un système particulier de n solutions indépendantes. Un tel système peut se déduire des considérations du n° 3. Supposons que le déterminant Δ ne soit pas nul, alors on a le système suivant de n solutions indépendantes

$$\begin{matrix} \Delta_{1,m+1}, & \Delta_{2,m+1}, & \dots, & \Delta_{m,m+1}, & -\Delta, & 0, & 0, & \dots, & 0, \\ \Delta_{1,m+2}, & \Delta_{2,m+2}, & \dots, & \Delta_{m,m+2}, & 0, & -\Delta, & 0, & \dots, & 0, \\ \dots\dots, & \dots\dots, & \dots, & \dots\dots, & ., & \dots, & ., & \dots, & ., \\ \Delta_{1,m+n}, & \Delta_{2,m+n}, & \dots, & \Delta_{m,m+n}, & 0, & 0, & 0, & \dots, & -\Delta \end{matrix}$$

En effet, ce sont là bien n solutions, car on a [form. (4) du n° 3]

$$a_{i,1}\Delta_{1,m+k} + a_{i,2}\Delta_{2,m+k} + \dots + a_{i,m}\Delta_{m,m+k} - a_{i,m+k}\Delta = 0.$$

Ces solutions sont indépendantes, car l'un des déterminants est $(-\Delta)^n$.

Et si l'on considère maintenant les déterminants de cette matrice qui correspondent aux $mn+1$ déterminants que nous avons considérés dans le n° 3, on reconnaît immédiatement qu'ils n'en diffèrent que par le facteur $(-1)^n \Delta^{n-1}$, et cette proportionnalité s'étend aisément aux autres déterminants.

Plus généralement, on peut obtenir n solutions indépendantes ainsi. Soit

$$D = \begin{vmatrix} a_{1,1} & \dots & a_{1,m+n} \\ \dots & \dots & \dots\dots \\ a_{m,1} & \dots & a_{m,m+n} \\ c_{1,1} & \dots & c_{1,m+n} \\ \dots & \dots & \dots\dots \\ c_{n,1} & \dots & c_{n,m+n} \end{vmatrix}.$$

Puisque tous les déterminants de la matrice donnée ne sont pas nuls, on pourra choisir les nombres $c_{i,k}$, de manière que D ne soit pas nul. Désignant alors par $C_{i,k}$ le coefficient de $c_{i,k}$ dans D, il est clair que l'on a le système suivant de n solutions

$$\begin{matrix} C_{1,1}, & \dots, & C_{1,m+n}, \\ \dots, & \dots, & \dots\dots, \\ C_{n,1}, & \dots, & C_{n,m+n}, \end{matrix}$$

et, d'après un théorème connu, un déterminant quelconque de cette matrice est égal au déterminant correspondant de la matrice $\| a_{i,k} \|$ multiplié par D^{n-1}.

9. Nous allons résoudre maintenant le problème suivant. Étant donnée une matrice

$$\| A \|,$$

du type $n \times (m+n)$, dont d est le plus grand diviseur, trouver toutes les solutions de l'équation

$$\| A \| = \| C \| \times \| B \|,$$

le déterminant $| C |$ étant $\pm d$. Il est clair que le plus grand diviseur de $\| B \|$ est 1, et si l'on a trouvé une matrice dont les déterminants sont proportionnels à ceux de $\| A \|$ et dont le plus grand diviseur est $= 1$, on pourra la prendre pour $\| B \|$; la matrice $\| C \|$ s'en déduit d'après le théorème VI.

On peut obtenir une telle matrice $\| B \|$ en considérant le système indéterminé dont la matrice est $\| A \|$. On cherchera m solutions indépendantes formant une matrice $\| A' \|$. Ensuite, on cherche un système fondamental de solutions du système indéterminé dont la matrice est $\| A' \|$. La matrice formée par ce système fondamental satisfait évidemment aux conditions.

Mais voici une autre méthode qui sera préférable ordinairement. Divisons d'abord la première ligne horizontale de $\| A \|$ par le plus grand commun diviseur des nombres qu'elle renferme, on aura ainsi la matrice

$$\begin{matrix} b_{1,1}, & b_{1,2}, & \dots, & b_{1,m+n}, \\ a_{2,1}, & a_{2,2}, & \dots, & a_{2,m+n}, \\ \dots, & \dots, & \dots, & \dots\dots, \\ a_{n,1}, & a_{n,2}, & \dots, & a_{n,m+n}. \end{matrix}$$

Soit maintenant d_1 le plus grand commun diviseur de la matrice formée avec les deux premières lignes. Je dis que l'on pourra déterminer un nombre x satisfaisant aux congruences

$$x b_{1,i} \equiv a_{2,i} \pmod{d_1},$$
$$i = 1, 2, \ldots, m - n.$$

C'est ce qui résulte du théorème V. En retranchant donc de la seconde ligne, la première multipliée par x, elle deviendra divisible par d_1 et, après la division, on aura une matrice

$$\begin{matrix} b_{1,1}, & b_{1,2}, & \ldots, & b_{1,m+n}, \\ b_{2,1}, & b_{2,2}, & \ldots, & b_{2,m+n}, \\ a_{3,1}, & a_{3,2}, & \ldots, & a_{3,m+n}, \end{matrix}$$

et le plus grand diviseur de la matrice des deux premières lignes est $= 1$.

Soit d_2 le plus grand diviseur de la matrice des trois premières lignes, les congruences

$$x b_{1,i} + y b_{2,i} \equiv a_{3,i} \pmod{d_2},$$
$$(i = 1, 2, \ldots, m + n)$$

admettent encore une solution, d'après le théorème V. En retranchant de la troisième ligne la première multipliée par x et la seconde ligne multipliée par y, on pourra diviser par d_2 et, dans la matrice obtenue

$$\begin{matrix} b_{1,1}, & b_{1,2}, & \ldots, & b_{1,m+n}, \\ b_{2,1}, & b_{2,2}, & \ldots, & b_{2,m+n}, \\ b_{3,1}, & b_{3,2}, & \ldots, & b_{3,m+n}, \\ a_{4,1}, & a_{4,2}, & \ldots, & a_{4,m+n}, \end{matrix}$$

le plus grand diviseur de la matrice partielle formée par les trois premières lignes est $= 1$. Il est clair que l'on peut continuer ainsi, on finira par trouver une matrice

$$\| b_{i,k} \| = \| \mathrm{B} \|$$
$$\begin{pmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, n + m \end{pmatrix}^2$$

dont le plus grand diviseur est $= 1$, et il est clair que ses déterminants seront proportionnels à ceux de $\| \mathrm{A} \|$. On peut remarquer que ce procédé donne, dans le cas $m = 0$, une nouvelle méthode pour la construction d'un déterminant $= \pm 1$.

Ayant ainsi obtenu une solution particulière

$$\| \mathrm{A} \| = \| \mathrm{C} \| \cdot \| \mathrm{B} \|.$$

il est facile de voir que la solution la plus générale sera comprise dans les formules

$$\| A \| = \| C_0 \| \times \| B_0 \|,$$

où

$$\| B_0 \| = \| E \| \times \| B \|,$$
$$\| C_0 \| = \| C \| \times \| E \|^{-1},$$

$\| E \|$ étant une matrice quelconque du type $n \times n$ dont le déterminant est ± 1.

Lorsque $\| A \|$ est la matrice de n solutions indépendantes du système (1), la matrice $\| B \|$ sera composée d'un système fondamental de solutions.

10. On peut obtenir la solution du système

$$(1) \qquad \begin{cases} a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n} = 0, \\ i = 1, 2, \ldots, m \end{cases}$$

encore par une autre méthode, un peu différente de celle que nous avons exposée dans le n° 4, et qui conduit à un résultat dont nous aurons besoin plus loin.

Nous avons vu, dans le Chapitre II, que par une substitution linéaire de déterminant ± 1, on peut transformer l'expression

$$a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,m+n}x_{m+n}$$

en $d_1 x'_1$, d_1 étant le plus grand commun diviseur des coefficients $a_{1,1}, \ldots, a_{1,m+n}$.

A l'aide de cette transformation, on déduira de (1) un système équivalent dont la matrice affectera la forme

$$\begin{matrix} d_1 & 0 & \ldots & 0 \\ a'_{2,1} & a'_{2,2} & \ldots & a'_{2,m+n} \\ \ldots & \ldots & \ldots & \ldots \\ a'_{m,1} & a'_{m,2} & \ldots & a'_{m,m+n}. \end{matrix}$$

Les coefficients $a'_{2,2}, a'_{2,3}, \ldots, a'_{2,m+n}$ ne peuvent pas être tous nuls, car tous les mineurs du second degré des deux premières lignes seraient nuls ; la même chose aurait lieu pour la matrice des $a_{i,k}$, ce qui est contre l'hypothèse admise. En opérant donc sur les variables $x'_2, x'_3, \ldots, x'_{m+n}$, on pourra transformer encore le système de manière à obtenir un nouveau système dont la matrice affecte la forme

$$\begin{matrix} d_1 & 0 & 0 & \ldots & 0 \\ a''_{2,1} & d_2 & 0 & \ldots & 0 \\ a''_{3,1} & a''_{3,2} & a''_{3,2} & \ldots & a''_{m+n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a''_{m,1} & a''_{m,2} & a''_{m,3} & \ldots & a''_{m,m+n} \end{matrix}$$

d_2 étant le p. g. c. d. de $a'_{2,2}, a'_{2,3}, \ldots, a'_{2,m+n}$. En continuant ainsi, on sera amené finalement à une matrice de la forme

$$(A) \quad \left\{ \begin{array}{ccccccc} d_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \beta_{2,1} & d_2 & \ldots & 0 & 0 & \ldots & 0 \\ \beta_{3,1} & \beta_{3,2} & \ldots & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & . & \ldots & . \\ \beta_{m,1} & \beta_{m,2} & \ldots & \beta_{m,m-1}, d_m & . & \ldots & 0 \end{array} \right.$$

Il est clair qu'on aura $d = d_1 d_2 d_3 \ldots d_m$, et si les nouvelles inconnues sont $y_1, y_2, \ldots, y_{m+n}$, la solution la plus générale s'obtient en posant

$$y_1 = y_2 = y_3 = \ldots = y_m = 0,$$

tandis que $y_{m+1}, y_{m+2}, \ldots, y_{m+n}$ peuvent prendre toutes les valeurs entières de $-\infty$ à $+\infty$.

On peut simplifier encore le tableau (A). En remplaçant d'abord y_2 par $y_2 - cy_1$, il est clair qu'on peut faire en sorte que le coefficient $\beta_{2,1}$ devient positif, mais inférieur à d_2. En remplaçant ensuite y_3 par $y_3 - cy_2 - c'y_2$, on peut assujettir les coefficients $\beta_{3,1}, \beta_{3,2}$ aux limitations

$$0 \leqq \beta_{3,1} < d_3, \qquad 0 \leqq \beta_{3,2} < d_3.$$

On voit, en définitive, qu'il existe toujours une substitution de déterminant $= 1$, tel que le système transformé a une matrice de la forme particulière (A), où les coefficients $d_1, d_2, \ldots, d_m$ sont positifs et

$$0 \leqq \beta_{i,k} < d_i \qquad [k = 1, 2, \ldots, (i-1)]$$

(*voir* Hermite, *Journal de Crelle*, t. 41, p. 192). On verra facilement que cette forme réduite (A) est unique. La nature invariantive des coefficients du tableau (A) s'aperçoit aisément. D'abord il est clair que d_i est la plus petite valeur (sauf 0) que peut avoir l'expression

$$a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n},$$

$x_1, x_2, \ldots, x_{m+n}$ étant liés par les relations

$$a_{k,1}x_1 + a_{k,2}x_2 + \ldots + a_{k,m+n}x_{m+n} = 0,$$
$$k = 1, 2, 3, \ldots, (i-1).$$

Ensuite $\beta_{2,1}$ est la plus petite valeur que peut avoir la fonction linéaire

$$a_{2,1}x_1 + \ldots + a_{2,m+n}x_{m+n},$$

$x_1, \ldots, x_{m+n}$ étant liés par la relation

$$a_{1,1}x_1 + \ldots + a_{1,m+n}x_{m+n} = d_1.$$

Ensuite $\beta_{3,1}$, $\beta_{3,2}$ sont les plus petites valeurs de

$$a_{3,1}x_1 + \ldots + a_{3,m+n}x_{m+n},$$

$x_1, \ldots, x_{m+n}$ étant assujettis, dans le premier cas, aux relations

$$a_{1,1}x_1 + \ldots + a_{1,m+n}x_{m+n} = d_1,$$
$$a_{2,1}x_1 + \ldots + a_{2,m+n}x_{m+n} = \beta_{2,1}$$

et, dans le second cas, aux relations

$$a_{1,1}x_1 + \ldots + a_{1,m+n}x_{m+n} = 0,$$
$$a_{2,1}x_1 + \ldots + a_{2,m+n}x_{m+n} = d_2,$$

ainsi de suite.

11. Considérons maintenant le système non homogène

(III) $$a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n} = a_i$$
$$(i = 1, 2, \ldots, m).$$

Soit d le plus grand diviseur de la matrice de ce système, d' le plus grand diviseur de la matrice complétée, il est clair que d' divise d. Mais, en éliminant $m-1$ des inconnues, on reconnaît que tout déterminant de la matrice complétée, qui n'est pas en même temps un déterminant de la matrice non complétée, doit être divisible par d. Pour que le système (III) admette des solutions, il est donc nécessaire que l'on ait $d = d'$. Mais cette condition est aussi suffisante.

Théorème VIII. — *Pour que le système* (III) *admette des solutions, il faut et il suffit que le plus grand diviseur de la matrice du système soit égal au plus grand diviseur de la matrice complétée.*

En effet, dire que le système (III) admet une solution, c'est la même chose que de dire que le système homogène

$$a_i x_0 + a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n} = 0$$

admet une solution où $x_0 = -1$. Or la solution générale du système homogène est

$$x_i = \beta_{0,i}t_0 + \beta_{1,i}t_1 + \ldots + \beta_{n,i}t_n,$$
$$i = 0, 1, 2, \ldots, (m+n).$$

En supposant $d = d'$ les déterminants de la matrice des $\| \beta_{i,k} \|$ qui renferment

les coefficients $\beta_{0,0}$, $\beta_{1,0}$, ..., $\beta_{n,0}$ sont égaux aux déterminants correspondants de la matrice du système homogène, divisés par d. Mais ces déterminants sont simplement les déterminants du système (III), et en les divisant par d on obtient des nombres dont le p. g. c. d. est $= 1$. Il est clair par là que le p. g. c. d. de $\beta_{0,0}$, $\beta_{1,0}$, ..., $\beta_{n,0}$ est aussi $= 1$, et, par conséquent, on peut donner à t_0, t_1, ..., t_m des valeurs telles que $x_0 = -1$. On reconnaîtrait aussi facilement la vérité de ce théorème à l'aide de la méthode de réduction du n° 4. On voit, d'après ce théorème, que si l'on considère l'ensemble des solutions du système homogène (I), la plus petite valeur de x_k (sauf o) est $\frac{d_k}{d}$, d_k étant le plus grand diviseur de la matrice obtenue en supprimant la $k^{\text{ième}}$ colonne. Cette valeur $\frac{d_k}{d}$ est donc, dans tout système fondamental de solutions

$$\beta_{i,1}, \beta_{i,2}, \ldots, \beta_{i,m+n},$$
$$i = 1, 2, \ldots, n$$

le p. g. c. d. de $\beta_{1,k}$, $\beta_{2,k}$, ..., $\beta_{n,k}$.

Il est clair que pour obtenir la solution la plus générale du système non homogène (III), il suffit d'ajouter à une solution particulière la solution la plus générale du système homogène (I).

12. Si le système (III) admet une solution pour certaines valeurs de u_1, u_2, ..., u_m, il en sera de même encore si l'on remplace ces nombres par v_1, v_2, ..., v_m, où

$$u_i \equiv v_i \pmod{d}, \qquad i = 1, 2, \ldots, m.$$

La possibilité ou l'impossibilité du système ne dépend donc que des résidus de u_1, u_2, ..., u_m par rapport à d. Le nombre total de ces systèmes de résidus est de d^m, mais pour d^{m-1} de ces systèmes seulement, les équations (III) admettent une solution. Pour le reconnaître, il suffit de recourir à la transformation du n° **10**, qui donne un système équivalent de la forme

$$\begin{aligned}
u_1 &= d_1 y_1,\\
u_2 &= \beta_{2,1} y_1 + d_2 y_2,\\
u_3 &= \beta_{3,1} y_1 + \beta_{2,2} y_2 + d_3 y_3,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
u_m &= \beta_{m,1} y_1 + \ldots + \beta_{m,m-1} y_{m-1} + d_m y_m,
\end{aligned}$$
$$d_1 d_2 \ldots d_m = d$$

Il est clair d'abord que u_1 ne peut voir que $\frac{d}{d_1}$ valeurs par rapport au module d.

A chacune de ces valeurs de u_1 correspond une valeur déterminée de y_1 et ensuite évidemment $\frac{d}{d_2}$ valeurs de u_2 par rapport au module d. A chaque système de valeurs de u_1 et u_2 correspondent ensuite des valeurs déterminées de y_1 et y_2 et ensuite $\frac{d}{d_3}$ valeurs de u_3 par rapport au module d, etc. Le nombre total des systèmes de résidus de $u_1, u_2, \ldots, u_m$, par rapport au module d, est donc

$$\frac{d}{d_1} \times \frac{d}{d_2} \times \ldots \times \frac{d}{d_m} = d^{m-1}. \qquad \text{C. Q. F. D.}$$

Parmi les valeurs admissibles pour u_i figure toujours la valeur $u_i = 0$, et si l'on se donne d'avance

$$u_1 = u_2 = \ldots = u_k = 0,$$

les $u_{k+1}, \ldots, u_m$ ne peuvent plus représenter que d^{m-k} systèmes de résidus par rapport au module d. Mais, en raisonnant comme tout à l'heure, on voit que, parmi ces systèmes, il n'y en a que

$$\frac{d^{m-k}}{d_{k+1}, d_{k+2}, \ldots, d_m} = d_1 d_2 \ldots d_k \times d^{m-k-1},$$

pour lesquels le système (III) admet des solutions. Il est clair que $d_1 d_2 \ldots d_k$ est ici le plus grand diviseur de la matrice des k premières des équations (III).

13. Ces propositions ont lieu encore dans le cas $n = 0$, lorsque le nombre des équations est égal au nombre des inconnues, et nous allons en faire une application dans un cas de cette nature.

Prenons un système de m^2 nombres entiers

$$a_{i,k} \qquad (i, k = 1, 2, \ldots, m),$$

dont le déterminant

$$\Delta = |a_{i,k}|$$

est positif > 0.

Si l'on considère les équations

$$\text{(A)} \qquad \frac{\partial\Delta}{\partial a_{i,1}} x_1 + \frac{\partial\Delta}{\partial a_{i,2}} x_2 + \ldots + \frac{\partial\Delta}{\partial a_{i,m}} x_m = u_i,$$
$$i = 1, 2, \ldots, m,$$

le déterminant est Δ^{m-1}, et, d'après ce qu'on vient de voir, il y a $\Delta^{(m-1)^2}$ systèmes de résidus u_i par rapport au module Δ^{m-1} pour lesquels le système (A) admet une solution entière. Mais la solution de ce système est donnée par les formules

$$\Delta x_i = a_{1,i} u_1 + a_{2,i} u_2 + \ldots + a_{m,i} u_m,$$
$$i = 1, 2, \ldots, m$$

On voit donc que si le système a une solution entière pour un système de valeurs de $u_1, \ldots, u_m$, il en aura encore une en remplaçant u_i par $v_i \equiv u_i \pmod{\Delta}$. Soit k le nombre des systèmes de résidus des u_i par rapport au module Δ, pour lesquels les équations (A) admettent une solution, un tel système en engendrera évidemment $\Delta^{m(m-2)}$ par rapport au module Δ^{m-1}; donc

$$k \times \Delta^{m(m-2)} = \Delta^{(m-1)^2},$$
$$k = \Delta.$$

Il est clair, du reste, que ce nombre k est simplement le nombre des solutions des congruences

$$a_{1,i}\, u_1 + a_{2,i}\, u_2 + \ldots + a_{m,i}\, u_m \equiv 0 \pmod{\Delta},$$

et, d'après un théorème que nous rencontrerons plus loin, on peut conclure de là aussi cette valeur $k = \Delta$.

Ce résultat peut s'énoncer ainsi :

Théorème IX. — *Il y a exactement* Δ *systèmes de nombres entiers* $x_1, x_2, \ldots, x_m$ *qui satisfont aux inégalités*

$$0 \leqq \frac{\partial \Delta}{\partial a_{i,1}} x_1 + \frac{\partial \Delta}{\partial a_{i,2}} x_2 + \ldots + \frac{\partial \Delta}{\partial a_{i,m}} x_m < \Delta$$
$$(i = 1, 2, \ldots, m).$$

Dans les cas $m = 2$, $m = 3$, ce théorème admet une interprétation géométrique très simple. Considérons dans l'espace trois axes rectangulaires OX, OY, OZ et le réseau de tous les points dont les trois coordonnées x, y, z sont des nombres entiers. Soient

$$A(x_1, y_1, z_1), \qquad B(x_2, y_2, z_2), \qquad C(x_3, y_3, z_3)$$

trois points du réseau; nous supposerons que

$$\Delta = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}$$

soit différent de zéro et positif. Alors Δ est le volume d'un parallélépipède dont trois arêtes sont OA, OB, OC. Soient O_1, A_1, B_1, C_1 les sommets du parallélépipède opposés à O, A, B, C.

L'équation de la face OBC est

$$\frac{\partial \Delta}{\partial x_1} X + \frac{\partial \Delta}{\partial y_1} Y + \frac{\partial \Delta}{\partial z_1} Z = 0,$$

et l'équation de la face opposée $O_1B_1C_1$ passant par le sommet O_1 est

$$\frac{\partial\Delta}{\partial x_1}X + \frac{\partial\Delta}{\partial y_1}Y + \frac{\partial\Delta}{\partial z_1}Z = \Delta.$$

Les trois inégalités

$$0 \leqq \frac{\partial\Delta}{\partial x_1}X + \frac{\partial\Delta}{\partial y_1}Y + \frac{\partial\Delta}{\partial z_1}Z < \Delta,$$
$$0 \leqq \frac{\partial\Delta}{\partial x_2}X + \frac{\partial\Delta}{\partial y_2}Y + \frac{\partial\Delta}{\partial z_2}Z < \Delta,$$
$$0 \leqq \frac{\partial\Delta}{\partial x_3}X + \frac{\partial\Delta}{\partial y_3}Y + \frac{\partial\Delta}{\partial z_3}Z < \Delta$$

expriment donc que le point X, Y, Z est à l'intérieur du parallélépipède ou sur l'une des faces passant par O, mais non sur une des faces passant par O_1. Le théorème IX exprime donc qu'il y a exactement Δ points du réseau qui satisfont à ces conditions. Une légère attention suffit pour reconnaître que, dans ce dénombrement, il ne faut compter qu'un des huit sommets du parallélépipède : c'est le sommet O. Quant aux points sur les arêtes (mais qui ne sont pas des sommets), il ne faut compter que les points qui sont sur les trois arêtes passant par O. Enfin, pour les points sur les faces (mais non sur une arête), il ne faut compter que ceux qui sont sur les trois faces passant par O, mais non ceux qui sont sur les trois autres faces.

Il est clair qu'on obtiendrait le même nombre Δ, en comptant tous les points sur les faces, arêtes, sommets, si l'on adopte cette règle de compter un sommet pour $\frac{1}{8}$, un point sur une arête pour $\frac{1}{4}$, un point sur une face pour $\frac{1}{2}$.

Il serait extrêmement facile de démontrer directement ce résultat en prolongeant les arêtes OA, OB, OC jusqu'en A', B', C', de telle manière que

$$OA' = k.OA, \qquad OB' = k.OB, \qquad OC' = k.OC,$$

k étant un entier, et en considérant alors le parallélépipède avec les arêtes OA', OB', OC'. Le rapport des volumes des deux parallélépipèdes est k^3, et l'on reconnaît aussi que le rapport des nombres des points du réseau à l'intérieur des deux parallélépipèdes (comptés d'après la règle indiquée) est aussi exactement k^3. Or, d'après la définition même du volume, le rapport du volume et du nombre des points à l'intérieur du parallélépipède OA'B'C' doit tendre vers 1 pour $k = \infty$. Mais puisque ce rapport ne varie pas, il est toujours $= 1$.

On peut se placer à un point de vue un peu différent. Considérons dans l'espace le réseau des points dont les coordonnées sont des multiples de $\frac{1}{k}$, k étant un nombre entier. Le *volume* d'une certaine partie de l'espace peut être défini

alors (d'après Lejeune-Dirichlet) comme la limite du rapport

$$M : k^3$$

pour $k = \infty$, M étant le nombre des points du réseau qui appartiennent à la partie de l'espace que l'on considère. Adoptant cette définition de volume, on peut conclure directement du théorème IX que le *volume* du parallélépipède OABC est exprimé par le déterminant Δ.

On comprendra maintenant que M. Smyth a pu déduire de ces considérations une démonstration arithmétique de la formule de transformation des intégrales multiples.

Solutions de quelques problèmes sur les matrices.

14. Étant donnée une matrice

$$a_1, a_2, \ldots, a_{n+1} \quad \text{ou} \quad \| A \|$$

du type $1 \times (n+1)$, dont d est le plus grand diviseur, nous avons vu (Chap. II, 22) qu'on peut trouver toujours une matrice

$$\| b_{i,k} \| \quad \text{ou} \quad \| B \| \qquad \begin{pmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, n+1 \end{pmatrix}$$

du type $n\,(n+1)$, telle que le déterminant

$$\begin{vmatrix} A \\ B \end{vmatrix} = d.$$

Proposons-nous maintenant de trouver la solution la plus générale de ce problème. Il est clair, en divisant tous les éléments de $\| A \|$ par d, qu'on peut supposer $d = 1$. Cela étant, si l'on a

$$\begin{vmatrix} A \\ B \end{vmatrix} = 1, \qquad \begin{vmatrix} A \\ C \end{vmatrix} = 1,$$

$\| C \|$ étant une solution quelconque, nous savons, par le théorème VI, qu'il existe toujours une matrice $\| E \|$ du type $(n+1) \times (n+1)$ (et une seule), telle que

$$(1) \qquad \left\| \begin{matrix} A \\ C \end{matrix} \right\| = \| E \| \times \left\| \begin{matrix} A \\ B \end{matrix} \right\|,$$

où $| E | = \pm 1$. Mais il est clair que la matrice $\| E \|$ doit avoir ici la forme particulière

$$\begin{matrix} 1 & 0 & 0 & \ldots & 0 \\ p_1 & e_{1,1} & e_{1,2} & \ldots & e_{1,n} \\ p_2 & e_{2,1} & e_{2,2} & \ldots & e_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_n & e_{n,1} & e_{n,2} & \ldots & e_{n,n} \end{matrix}$$

$p_1, p_2, \ldots, p_n$ étant arbitraires et $|e_{i,k}| = \pm 1$. Avec cette expression de $\|E\|$, la formule (1) renferme donc toutes les solutions du problème et chaque solution une seule fois. On peut mettre cette solution sous une autre forme en remarquant que la matrice $\|E\|$ peut se mettre sous la forme

$$\begin{Vmatrix} 1 & . & \ldots & 0 \\ 0 & e_{1,1} & \ldots & e_{1,n} \\ . & \ldots & \ldots & \ldots \\ 0 & e_{n,1} & \ldots & e_{n,n} \end{Vmatrix} \times \begin{Vmatrix} 1 & 0 & 0 & \ldots & 0 \\ q_1 & 1 & 0 & \ldots & 0 \\ q_2 & 0 & 1 & \ldots & 0 \\ .. & . & . & \ldots & . \\ q_n & 0 & 0 & \ldots & 1 \end{Vmatrix},$$

$q_1, q_2, \ldots, q_n$ étant des nombres qui peuvent avoir des valeurs arbitraires. En substituant cette expression dans la formule (1), on obtient sans difficulté la matrice la plus générale $\|C\|$ qui satisfait au problème, sous la forme

$$\|C\| = \|e_{i,k}\| \times \|b_{i,k} + q_i a_k\|,$$

$\|B\| = \|b_{i,k}\|$ étant une solution particulière.

15. Plus généralement, soit

$$\|a_{i,k}\| \quad \text{ou} \quad \|A\| \qquad \begin{bmatrix} i = 1, 2, \ldots, m \\ k = 1, 2, \ldots, (m+n) \end{bmatrix}$$

une matrice donnée du type $m \times (m+n)$, dont d est le plus grand diviseur. Proposons-nous de trouver toutes les matrices

$$\|c_{i,k}\| \quad \text{ou} \quad \|C\| \qquad \begin{bmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, (m+n) \end{bmatrix}$$

du type complémentaire $n \times (m+n)$ telles que

$$\begin{vmatrix} A \\ C \end{vmatrix} = \pm d.$$

On peut remarquer d'abord qu'on peut supposer $d = 1$, car nous savons qu'on peut trouver une matrice $\|A'\|$ du même type que $\|A\|$, dont les déterminants sont proportionnels à ceux de $\|A\|$ et dont le plus grand diviseur est $= 1$ (n° 9). Cette matrice $\|A'\|$ étant obtenue, il est clair que les deux conditions

$$\begin{vmatrix} A \\ C \end{vmatrix} = \pm d, \qquad \begin{vmatrix} A' \\ C \end{vmatrix} = \pm 1$$

sont absolument équivalentes. Nous supposerons donc $d = 1$, et de plus qu'on ait obtenu déjà une solution particulière

$$\|b_{i,k}\| \quad \text{ou} \quad \|B\| \qquad \begin{bmatrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, (m+n) \end{bmatrix}.$$

Ayant

$$\begin{vmatrix} A \\ C \end{vmatrix} = \pm 1, \qquad \begin{vmatrix} A \\ B \end{vmatrix} = \pm 1,$$

on en conclut encore par le théorème VI

$$(1) \qquad \begin{Vmatrix} A \\ C \end{Vmatrix} = \| E \| \times \begin{Vmatrix} A \\ B \end{Vmatrix},$$

$\| E \|$ étant une matrice du type $(m+n)\times(m+n)$ dont le déterminant est $= \pm 1$. Mais il est clair que cette matrice $\| E \|$ doit avoir ici la forme particulière

$$\begin{matrix} 1 & 0 & \dots & 0 & 0 & . & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & . & \dots & 0 \\ . & . & \dots & . & . & . & \dots & . \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ p_{1,1} & p_{1,2} & \dots & p_{1,m} & e_{1,1} & e_{1,2} & \dots & e_{1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ p_{n,1} & p_{n,2} & \dots & p_{n,m} & e_{n,1} & e_{n,2} & \dots & e_{n,n}. \end{matrix}$$

Cette formule (1) renferme ainsi déjà la solution la plus générale du problème, mais on peut la mettre encore sous une autre forme en remarquant que la matrice $\| E \|$ peut se mettre sous la forme d'un produit

$$\begin{Vmatrix} 1 & 0 & \dots & 0 & . & \dots & 0 \\ 0 & 1 & \dots & . & . & \dots & 0 \\ . & . & \dots & . & . & \dots & . \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & e_{1,1} & \dots & e_{1,n} \\ . & . & \dots & . & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & e_{n,1} & \dots & e_{n,n} \end{Vmatrix} \times \begin{Vmatrix} 1 & . & \dots & . & . & . & \dots & 0 \\ 0 & 1 & \dots & 0 & . & . & \dots & 0 \\ . & . & \dots & . & . & . & \dots & . \\ 0 & 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ q_{1,1} & q_{1,2} & \dots & q_{1,m} & 1 & . & . & 0 \\ \dots & \dots & \dots & \dots & . & . & \dots & . \\ q_{n,1} & q_{n,2} & \dots & q_{n,m} & 0 & 0 & \dots & 1 \end{Vmatrix},$$

où les $q_{i,k}$ peuvent avoir des valeurs quelconques. On obtient facilement

$$\| C \| = \begin{Vmatrix} e_{1,1} & \dots & e_{1,n} \\ \dots & \dots & \dots \\ e_{n,1} & \dots & e_{n,n} \end{Vmatrix} \times \| b_{i,k} + q_{i,1}a_{1,k} + q_{i,2}a_{2,k} + \dots + q_{i,m}a_{m,k} \|$$

$$\begin{bmatrix} i = 1, 2, \dots, n \\ k = 1, 2, \dots, (m+n) \end{bmatrix},$$

où les $e_{i,k}$ doivent satisfaire à la relation $| e_{i,k} | = \pm 1$.

Pour obtenir la solution particulière $\| B \|$, on prendra d'abord une matrice quelconque $\| m_{i,k} \|$ ou $\| M \|$ du type $n \times (m+n)$, telle que le déterminant de la

matrice

$$\begin{Vmatrix} A \\ M \end{Vmatrix}$$

ne soit pas nul. Par le procédé du n° 9 on pourra, sans changer les m premières lignes, en déduire une autre matrice du même type $(m+n)\times(m+n)$ et dont le déterminant est ± 1.

16. Nous avons vu (Chap. II, n° 21) qu'on peut toujours trouver une matrice du type $n\times(n+1)$ dont les déterminants ont des valeurs données, non toutes nulles. On peut se proposer d'obtenir *toutes* les matrices qui satisfont à ces conditions, mais nous traiterons directement le problème plus général :

Trouver toutes les matrices du type $m\times(m+n)$ dont les déterminants ont des valeurs données.

A cause des relations identiques entre les déterminants, les valeurs données ne peuvent pas être quelconques. Adoptons les notations du n° 3 et supposons que le déterminant Δ ne soit pas nul : on pourra se borner à considérer les $mn+1$ déterminants Δ, $\Delta_{i,m+k}$. Ces déterminants-là ne peuvent pas même être des nombres arbitraires, il faut que les autres déterminants Δ' qu'on en déduit par la formule (5) du n° 3 soient aussi des entiers. Mais, cela étant, nous allons voir que le problème est toujours possible et admet une infinité de solutions.

En effet, prenons d'abord arbitrairement les m premières colonnes avec la seule condition

$$|a_{i,k}| = \Delta \qquad (i, k = 1, 2, \ldots, m),$$

alors on pourra déterminer les autres colonnes comme au n° 3; il est vrai que ces autres éléments

$$a_{i,m+k} = (a_{i,1}\Delta_{1,m+k} + a_{i,2}\Delta_{2,m+k} + \ldots + a_{i,m}\Delta_{m,m+k}) : \Delta$$

ne seront pas des entiers; toujours est-il vrai que la matrice ainsi formée admettra pour déterminants les valeurs données, qui sont toutes entières. En multipliant les lignes horizontales par Δ, on obtiendra une matrice dont les déterminants sont proportionnels aux valeurs données. On peut alors déduire de là (par le procédé du n° 9) une autre matrice dont les déterminants sont encore proportionnels aux valeurs données, mais dont le plus grand diviseur est 1. Soit

$$\|B\|$$

cette matrice, si d est le p. g. c. d. de tous les déterminants de la matrice cherchée, l'expression la plus générale de cette matrice sera

$$\|C\| \times \|B\|,$$

où $\| C \|$ est une matrice quelconque du type $m \times m$, dont le déterminant est $= \pm d$. En prenant en particulier pour les $a_{i,k}$ $(i,k = 1, \ldots, m)$ les valeurs suivantes

$$a_{1,1} = a_{2,2} = \ldots = a_{m-1,m-1} = 1, \qquad a_{m,m} = \Delta.$$
$$a_{i,k} = 0, \qquad i > k,$$

on trouve que les déterminants de la matrice

$$\begin{array}{cccccccc} \Delta & 0 & \ldots & 0 & \Delta_{1,m+1} & \Delta_{1,m+2} & \ldots & \Delta_{1,m+n}, \\ 0 & \Delta & \ldots & 0 & \Delta_{2,m+1} & \Delta_{2,m+2} & \ldots & \Delta_{2,m+n}, \\ . & . & \ldots & . & \ldots & \ldots & \ldots & \ldots, \\ 0 & 0 & \ldots & \Delta & \Delta_{m,m+1} & \Delta_{m,m+2} & \ldots & \Delta_{m,m+n} \end{array}$$

sont proportionnels aux déterminants de la matrice cherchée; on pourra donc en déduire la matrice $\| B \|$.

Si l'un des déterminants donnés divise exactement tous les autres, on le prendra pour Δ; dans ce cas, on peut écrire la matrice $\| B \|$ sans aucun calcul.

Une autre méthode pour trouver cette matrice $\| B \|$ est la suivante; considérons le système d'équations linéaires homogènes dont la matrice est

$$\begin{array}{cccccccc} \Delta_{1,m+1} & \Delta_{2,m+1} & \ldots & \Delta_{m,m+1} & -\Delta & 0 & \ldots & 0 \\ \Delta_{1,m+1} & \Delta_{2,m+2} & \ldots & \Delta_{m,m+2} & 0 & -\Delta & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & . & . & \ldots & . \\ \Delta_{1,m+n} & \Delta_{2,m+n} & \ldots & \Delta_{m,m+n} & 0 & 0 & \ldots & -\Delta \end{array}$$

La matrice formée par un système fondamental de solutions de ces équations sera une matrice du type $m \times (m+n)$; ses déterminants seront proportionnels aux valeurs données et le plus grand diviseur de cette matrice est $= 1$. C'est ce qui résulte immédiatement des propositions établies précédemment, si l'on se rappelle le théorème VII et sa démonstration.

17. Soit $\| A \| = \| a_{i,k} \|$ une matrice du type $m \times (m+n)$, dont le plus grand diviseur est δ, $\| C \| = \| c_{i,k} \|$ une matrice du type complémentaire $n \times (m+n)$, telle que

$$(1) \qquad \begin{vmatrix} a_{1,1} & \ldots & a_{1,m+n} \\ \ldots & \ldots & \ldots \\ a_{m,1} & \ldots & a_{m,m+n} \\ c_{1,1} & \ldots & c_{1,m+n} \\ \ldots & \ldots & \ldots \\ c_{n,1} & \ldots & c_{n,m+n} \end{vmatrix} = \pm \delta.$$

Nous savons qu'il existe de telles matrices (*voir* n° 15).

Soit ensuite $\|B\| = \|b_{i,k}\|$ une matrice du type $n \times (m+n)$, formée par un système fondamental de solutions des équations linéaires homogènes

$$a_{i,1}x_1 + \ldots + a_{i,m+n}x_{m+n} = 0 \qquad (i = 1, 2, \ldots, m).$$

Les matrices $\|B\|$ et $\|C\|$ sont du même type; à un déterminant Δ_b de la première on peut faire correspondre un déterminant Δ_c de la seconde, en supposant que deux déterminants correspondants sont formés avec n colonnes de même rang (et prises dans le même ordre) dans les deux matrices. Cela étant, on a

$$\sum \Delta_b \Delta_c = \pm 1,$$

la sommation s'étendant à toutes les paires de déterminants correspondants. Pour le montrer, remarquons que le plus grand diviseur de la matrice $\|B\|$ est l'unité : on peut donc former une matrice $\|D\| = \|d_{i,k}\|$ du type $m \times (m+n)$, telle que

$$(2) \qquad \begin{vmatrix} d_{1,1} & \ldots & d_{1,m+n} \\ \ldots & \ldots & \ldots \\ d_{m,1} & \ldots & d_{m,m+n} \\ b_{1,1} & \ldots & b_{1,m+n} \\ \ldots & \ldots & \ldots \\ b_{n,1} & \ldots & b_{n,m+n} \end{vmatrix} = \pm 1.$$

En multipliant les deux déterminants (1) et (2), il vient

$$\begin{vmatrix} A_{1,1} & \ldots & A_{m,1} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & . & \ldots & . \\ A_{1,m} & \ldots & A_{m,m} & 0 & \ldots & 0 \\ u_{1,1} & \ldots & u_{m,1} & v_{1,1} & \ldots & v_{n,1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ u_{1,n} & \ldots & u_{m,n} & v_{1,n} & \ldots & v_{n,n} \end{vmatrix} = \pm \delta.$$

$$A_{i,k} = a_{k,1}d_{i,1} + a_{k,2}d_{i,2} + \ldots + a_{k,m+n}d_{i,m+n},$$
$$v_{i,k} = b_{i,1}c_{k,1} + b_{i,2}c_{k,2} + \ldots + b_{i,m+n}c_{k,m+n},$$

c'est-à-dire

$$\begin{vmatrix} A_{1,1} & \ldots & A_{m,1} \\ \ldots & \ldots & \ldots \\ A_{1,m} & \ldots & A_{m,m} \end{vmatrix} \times \begin{vmatrix} v_{1,1} & \ldots & v_{n,1} \\ \ldots & \ldots & \ldots \\ v_{1,n} & \ldots & v_{n,n} \end{vmatrix} = \pm \delta.$$

Or, Δ_a et Δ_d étant deux déterminants correspondants des matrices $\|A\|$ et $\|D\|$

de même type, on a, d'après une propriété élémentaire des déterminants,

$$\begin{vmatrix} A_{1,1} & \dots & A_{m,1} \\ \dots & \dots & \dots \\ A_{1,m} & \dots & A_{m,m} \end{vmatrix} = \sum \Delta_a \Delta_d,$$

et de même

$$\begin{vmatrix} c_{1,1} & \dots & c_{n,1} \\ \dots & \dots & \dots \\ c_{1,n} & \dots & c_{n,n} \end{vmatrix} = \sum \Delta_b \Delta_c.$$

Mais tous les déterminants Δ_a sont divisibles par δ; on a donc nécessairement

$$\sum \Delta_a \Delta_d = \pm \delta, \qquad \sum \Delta_b \Delta_c = \pm 1, \qquad \text{C. Q. F. D.}$$

18. A l'aide de ce résultat, nous pouvons résoudre facilement le problème suivant : Étant donnée une matrice $\|A\|$ du type $m \times (m+n)$, dont le plus grand diviseur est δ, trouver toutes les matrices $\|D\|$ du même type et telles que

$$\sum \Delta_a \Delta_d = \pm \delta,$$

Δ_a et Δ_d étant deux déterminants correspondants des deux matrices. En effet, déterminons deux matrices $\|B\|$ et $\|C\|$ comme dans le numéro précédent. Si nous déterminons ensuite une matrice $\|D\|$ par la condition

$$\begin{vmatrix} D \\ B \end{vmatrix} = \pm 1,$$

nous savons que cette matrice fournit une solution de notre problème.

Mais je dis qu'on obtient ainsi *toutes* les solutions du problème. Soit, en effet, $\|D\|$ une solution quelconque, et posons

$$\begin{vmatrix} D \\ B \end{vmatrix} = k.$$

On en conclut

$$\begin{vmatrix} D \\ B \end{vmatrix} \times \begin{vmatrix} A \\ C \end{vmatrix} = \pm k\delta = \left(\sum \Delta_a \Delta_d\right) \times \left(\sum \Delta_b \Delta_c\right);$$

or on a, puisque $\|D\|$ est une solution,

$$\sum \Delta_a \Delta_d = \pm \delta,$$

et, d'après la proposition du n° 17,

$$\sum \Delta_b \Delta_c = \pm 1;$$

donc
$$k = \pm 1.$$

Il est clair par là que le problème proposé est identique avec le suivant que nous avons déjà résolu dans le nº 15 : Trouver toutes les matrices $\| D \|$, telles que

$$\begin{vmatrix} D \\ B \end{vmatrix} = \pm 1.$$

On obtient ces résultats aussi en s'appuyant sur le théorème VII, car la relation (1) du nº 17 peut s'écrire

$$\sum \Delta_a \Delta_c = \pm \delta.$$

Or, d'après le théorème cité, le rapport $\Delta_a : \Delta_b$ est constant et égal à $\pm \delta$; donc

$$\sum \Delta_b \Delta_c = \pm 1,$$

et, ensuite, il est évident que les relations

$$\sum \Delta_a \Delta_d = \pm \delta, \qquad \sum \Delta_b \Delta_d = \pm 1$$

sont équivalentes.

19. Nous terminerons ces considérations par quelques remarques sur le plus grand commun diviseur d'une matrice.

Dans le cas d'une matrice du type $1 \times n$, le plus grand diviseur peut être défini aussi comme la plus petite valeur (sauf 0) que peut prendre la fonction linéaire

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n,$$

pour les valeurs entières de $x_1, x_2, \ldots, x_n$. Il existe une proposition analogue pour une matrice $\| a_{i,k} \|$ du type $m \times (m+n)$. Considérons les m fonctions linéaires

$$X_i = a_{i,1} x_1 + a_{i,2} x_2 + \ldots + a_{i,m+n} x_{m+n}$$
$$(i = 1, 2, \ldots, m),$$

et m systèmes de valeurs de ces fonctions

$$X_{i,k} = a_{k,1} d_{i,1} + \ldots + a_{k,m+n} d_{i,m+n}$$
$$(i, k = 1, 2, \ldots, m),$$

le déterminant $| X_{i,k} |$ est toujours divisible par δ, le plus grand diviseur de la matrice $\| a_{i,k} \|$; mais nous savons, par l'analyse précédente, qu'on peut toujours choisir les $d_{i,k}$ de manière que ce déterminant devient égal à $\pm \delta$.

Par conséquent, δ est aussi la plus petite valeur (sauf o) que peut avoir le déterminant formé par m systèmes de valeurs des m fonctions linéaires X_i.

20. Soient $\| a_{i,k} \|$ ou $\| A \|$ une matrice du type $m \times (m+n)$, $\| A_p \|$ la matrice du type $m \times p$ formée par p colonnes de $\| A \|$. Nous supposons $p < m$. Désignons encore par d_p le plus grand diviseur de $\| A_p \|$, et par D le plus grand commun diviseur de tous les déterminants de $\| A \|$ qui renferment les p colonnes de $\| A_p \|$. Il est clair que D est est un multiple de d_p. Nous allons montrer *que tous les déterminants de* $\| A \|$ *sont divisibles par* $\frac{D}{d_p}$.

Pour simplifier un peu la démonstration, nous supposerons que $\| A_p \|$ est formée par les p premières colonnes de $\| A \|$. Nous avons à démontrer qu'un déterminant quelconque Δ de $\| A \|$ est divisible par $\frac{D}{d_p}$. Si ce déterminant Δ a un certain nombre r de colonnes communes avec $\| A_p \|$, nous pouvons encore supposer que ce sont les r premières colonnes de $\| A_p \|$. Cela étant, nous désignerons un déterminant quelconque de $\| A \|$ par le symbole

$$[\lambda_1, \lambda_2, \ldots, \lambda_m],$$

où $\lambda_1, \lambda_2, \ldots, \lambda_m$ indiquent les rangs des colonnes de $\| A \|$ qui figurent dans le déterminant.

En ajoutant à la matrice une $(m+1)^{\text{ième}}$ ligne

$$a_{i,1}, \quad a_{i,2}, \quad \ldots, \quad a_{i,m+n},$$

on obtient une matrice du type $(m+1) \times (m+n)$, dont tous les déterminants sont nuls. En développant un tel déterminant comme fonction linéaire des éléments de la dernière ligne, on aura, par exemple,

$$\begin{aligned}&[2, 3, \ldots, p, \lambda_1, \lambda_2, \ldots, \lambda_{m-p+1}]a_{i,1} + \ldots + [1, 2, \ldots, p-1, \lambda_1, \lambda_2, \ldots, \lambda_{m-p+1}]a_{i,p} \\ &+ [1, 2, \ldots, p, \lambda_2, \ldots, \lambda_{m-p+1}]a_{i,\lambda_1} + \ldots + [1, 2, \ldots, p_1, \lambda_1, \ldots, \lambda_{m-p}]a_{i,m-p+1} = 0.\end{aligned}$$

Les indices $\lambda_1, \lambda_2, \ldots$ sont ici et dans la suite toujours $> p$.

D'après notre notation, d_p est le plus grand diviseur de la matrice $\| A_p \|$, formée par les p premières colonnes de $\| A \|$. Il est clair, d'après cela, que ce qu'il faudra entendre par $d_{p-1}, d_{p-2}, \ldots, d_1$, ce sont les plus grands diviseurs de matrices que nous pouvons désigner par $\| A_{p-1} \|, \| A_{p-2} \|, \ldots, \| A_1 \|$. Dans l'identité que nous venons d'écrire, on peut prendre $i = 1, 2, \ldots, m$.

Si l'on élimine alors entre p des équations ainsi obtenues les quantités qui multiplient $a_{i,1}, a_{i,2}, \ldots, a_{i,p-1}$, il viendra

$$\begin{aligned}&[1, 2, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]\Delta_p \\ &+ [1, \ldots, p, \lambda_2, \ldots, \lambda_{m-p+1}]\Delta'_p + \ldots + [1, \ldots, p, \lambda_1, \ldots, \lambda_{m-p}]\Delta_p^{m-p+1} = 0.\end{aligned}$$

Ici Δ_p est un des déterminants de $\| \Lambda_p \|$, et il est clair que $\Delta_p^1, \Delta_p^2, \ldots, \Delta_p^{m-p+1}$ sont tous divisibles par d_{p-1}. Donc

$$[1, 2, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]\Delta_p$$

est divisible par $D \times d_{p-1}$. Mais Δ_p peut être un déterminant quelconque de $\| \Lambda_p \|$; par conséquent,

$$[1, 2, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]d_p$$

est aussi divisible par $D \times d_{p-1}$, c'est-à-dire

$$[1, 2, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]$$

est divisible par $\dfrac{D \times d_{p-1}}{d_p}$.

En laissant de côté maintenant la $p^{\text{ième}}$ colonne de $\| \Lambda \|$, on a les identités

$$\begin{gathered}[2, 3, \ldots, p-1, \lambda_1, \lambda_2, \ldots, \lambda_{m-p+2}]a_{i,1} + \ldots + [1, 2, \ldots, p-2, \lambda_1, \lambda_2, \ldots, \lambda_{m-p+2}]a_{i,p-1} \\ + [1, 2, \ldots, p-1, \lambda_2, \ldots, \lambda_{m-p+2}]a_{i,\lambda_1} + \ldots + [1, 2, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]a_{i,\lambda_{m-p+2}} = 0, \\ i = 1, 2, \ldots, m.\end{gathered}$$

En éliminant entre $p-1$ de ces relations les coefficients de $a_{i,1}, \ldots, a_{i,p-2}$, il vient

$$\begin{gathered}[1, 2, \ldots, p-2, \lambda_1, \ldots, \lambda_{m-p+2}]\Delta_{p-1} \\ + [1, 2, \ldots, p-1, \lambda_2, \ldots, \lambda_{m-p+2}]\Delta'_{p-1} + \ldots + [1, \ldots, p-1, \lambda_1, \ldots, \lambda_{m-p+1}]\Delta_{p-1}^{m-p+2} = 0,\end{gathered}$$

où Δ_{p-1} est un des déterminants de $\| \Lambda_{p-1} \|$ et où $\Delta_{p-1}^1, \ldots, \Delta_{p-1}^{m-p+2}$ sont tous divisibles par d_{p-2}. On voit donc que

$$[1, 2, \ldots, p-2, \lambda_1, \ldots, \lambda_{m-p+2}]\Delta_{p-1}$$

est divisible par $\dfrac{D \times d_{p-1} \times d_{p-2}}{d_p}$, et, puisque Δ_{p-1} peut être un déterminant quelconque de $\| \Lambda_{p-1} \|$, on en conclut que

$$[1, 2, \ldots, p-2, \lambda_1, \ldots, \lambda_{m-p+2}]d_{p-1},$$

doit être aussi divisible par le même nombre, c'est-à-dire

$$[1, 2, \ldots, p-2, \lambda_1, \ldots, \lambda_{m-p+2}]$$

est divisible par $\dfrac{D \times d_{p-2}}{d_p}$. En continuant ainsi, on reconnaît que

$$[1, 2, \ldots, r, \lambda_1, \lambda_2, \ldots, \lambda_{m-r}]$$

est divisible par $\frac{D}{d_p}=d_r$, et enfin que $[\lambda_1, \lambda_2, \ldots, \lambda_m]$ est divisible par $\frac{D}{d_p}$. La proposition énoncée est démontrée.

D'après la démonstration, on voit facilement que, si l'on suppose que tous les déterminants de $\| A \|$ ne sont pas nuls, les déterminants de $\| A \|$ qui renferment les p colonnes de $\| A_p \|$ ne peuvent pas être tous nuls, à moins que tous les déterminants de $\| A_p \|$ ne soient tous nuls. D et d_p sont alors indéterminés tous les deux.

Corollaire I. — Lorsque $d_p = 1$, D est le plus grand diviseur de la matrice $\| A \|$.

Corollaire II. — Lorsque le plus grand diviseur de la matrice $\| A \|$ est $= 1$, on a

$$D = d_p.$$

21. Considérons une matrice

$$\| B \| \quad \text{ou} \quad \| b_{i,k} \|,$$
$$i = 1, 2, \ldots, n,$$
$$k = 1, 2, \ldots, (m+n),$$

formée par un système fondamental de solutions de

$$a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n} = 0,$$
$$i = 1, 2, \ldots, m.$$

Soient $\| B_p \|$ une matrice formée par p des colonnes de $\| B \|$, en supposant $p < n$, d_p le plus grand diviseur de $\| B_p \|$. Soient ensuite δ le plus grand diviseur de la matrice des $a_{i,k}$, et δ_p le plus grand diviseur de la matrice obtenue en supprimant, dans la matrice des $a_{i,k}$, les p colonnes qui correspondent aux colonnes de $\| B_p \|$. Alors on peut énoncer le

Théorème X. — *Le plus grand diviseur d_p est égal à $\frac{\delta_p}{\delta}$.*

En effet, soient $\Delta, \Delta', \Delta'', \ldots$ les déterminants de $\| B \|$ qui renferment les p colonnes de $\| B_p \|$. Leur plus grand commun diviseur est d_p, d'après le corollaire II du n° 20. Mais on a d'autre part, d'après le théorème VII,

$$\Delta = \Theta : \delta, \qquad \Delta' = \Theta' : \delta, \qquad \Delta'' = \Theta'' : \delta, \qquad \ldots$$

$\Theta, \Theta', \Theta'', \ldots$ étant les déterminants de la matrice des $a_{i,k}$ qui correspondent aux déterminants $\Delta, \Delta', \Delta'', \ldots$. Mais il est évident que ces déterminants $\Theta, \Theta', \Theta'', \ldots$ sont précisément ceux dont le plus grand commun diviseur est δ_p, d'où la relation annoncée.

Il faut remarquer pourtant que tous les déterminants de la matrice $\|B_p\|$ peuvent s'annuler : d_p devient indéterminé alors. Mais il est clair que, dans ce cas, on a aussi

$$\mathfrak{D} = \mathfrak{D}' = \mathfrak{D}'' = \ldots = 0,$$

en sorte que δ_p devient indéterminé en même temps. Réciproquement, si δ_p devient indéterminé, il en est de même de d_p.

Nous avons supposé $p < n$, mais le théorème reste encore vrai dans le cas $p = n$; on retrouve alors un résultat connu (théorème VII).

L'énoncé du théorème se simplifie un peu dans le cas $\delta = 1$, et si l'on se rappelle l'espèce de réciprocité que nous avons signalée dans le n° 5, on verra que, dans ce cas, p peut avoir une valeur quelconque plus petite ou plus grande que n.

Systèmes de congruences linéaires.

22. Étant donné un système de m congruences entre n inconnues

$$(1) \qquad X_i = a_{i,1}x_1 + \ldots + a_{i,n}x_n \equiv 0 \pmod{M},$$

on peut en déduire un système équivalent, soit en opérant une substitution de déterminant ± 1 sur les inconnues $x_1, x_2, \ldots, x_n$, soit en remplaçant les m congruences données par m combinaisons

$$(2) \qquad X'_i = p_{i,1}X_1 + p_{i,2}X_2 + \ldots + p_{i,m}X_m \equiv 0 \pmod{M},$$
$$i = 1, 2, \ldots, m,$$

le déterminant des entiers $p_{i,k}$ étant encore ± 1, en sorte qu'on peut exprimer réciproquement les X_i par les X'_i.

En étudiant les équations linéaires indéterminées, nous avons employé exclusivement le premier moyen, la substitution de nouvelles inconnues ; mais ce n'est qu'en opérant à la fois par les deux méthodes qu'on peut obtenir la plus grande simplification possible.

En multipliant, dans le système (1), les premiers membres par $y_1, y_2, \ldots, y_m$ et ajoutant, on obtient la *forme bilinéaire*

$$F = \sum\sum a_{i,k}x_k y_i$$
$$\begin{pmatrix} i = 1, 2, \ldots, m \\ k = 1, 2, \ldots, n \end{pmatrix},$$

Nous dirons que cette forme bilinéaire correspond au système de congruences donné.

Une substitution linéaire sur les x, dans le système (1), conduira à un système transformé (1′), et il est clair que la forme bilinéaire qui correspond à ce système (1′) s'obtient simplement en effectuant directement la même substitution sur les x, dans la forme F.

D'autre part, si l'on remplace le système (1) par le système (2), on constate que la forme bilinéaire correspondante au système (2) s'obtient simplement en opérant dans la forme F la substitution

$$y_i = p_{1,i}\,y'_1 + p_{2,i}\,y'_2 + \ldots + p_{m,i}\,y'_m$$
$$(i = 1, 2, \ldots, m).$$

On voit par là que nous avons à étudier les différentes formes que peut prendre la forme F en opérant sur les variables x, y des substitutions de déterminants ± 1.

23. On appelle, en général, *forme* en Arithmétique un polynôme homogène de plusieurs indéterminées $x, y, z, \ldots$ à coefficients entiers. Si une telle forme F prend une certaine valeur m, pour certaines valeurs entières des indéterminées, on dit qu'elle *représente* le nombre m.

En effectuant dans F la substitution à coefficients entiers

$$\begin{aligned}
x &= a_1 x' + b_1 y' + c_1 z' + \ldots,\\
y &= a_2 x' + b_2 y' + c_2 z' + \ldots,\\
z &= a_3 x' + b_3 y' + c_3 z' + \ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,
\end{aligned}$$

on obtiendra une nouvelle forme F′, et l'on dit que F *renferme* F′, ou bien encore F′ est *contenue* dans F. Il est clair que tout nombre m qui peut être représenté par F′ peut être représenté aussi par F, mais la réciproque n'a pas lieu nécessairement.

Le cas particulier où le déterminant de la substitution que nous venons d'effectuer est égal à ± 1 est le plus important.

On peut alors exprimer réciproquement $x', y', z', \ldots$ comme fonctions linéaires à coefficients entiers de $x, y, z, \ldots$ et F est contenue aussi dans F′; on dit alors que les formes F et F′ sont *équivalentes*.

Il est évident que deux formes équivalentes représentent les mêmes nombres.

Ce qui caractérise une forme F dans ces considérations, ce sont ses coefficients; la notation des inconnues, au contraire, n'a aucune importance et l'on peut ainsi remplacer dans F′ les lettres $x', y', z', \ldots$ de nouveau par $x, y, z, \ldots$.

L'un des problèmes les plus importants qu'on a à résoudre est maintenant le suivant : Étant données deux formes F et F′, décider si elles sont équivalentes ou

non. Et, pour compléter la solution, il faudra encore trouver, dans le cas où il y a équivalence, toutes les substitutions qui transforment F en F'.

Plus généralement, on peut demander à reconnaître si F' est contenue dans F, mais nous nous bornerons ici à ajouter quelques remarques sur les conditions d'équivalence seulement.

Dans certains cas, la solution complète de ce problème se présente sous la forme suivante :

Pour que la forme F soit équivalente à F', il faut et il suffit que l'on ait

$$I_1 = I'_1, \qquad I_2 = I'_2, \qquad \ldots, \qquad I_k = I'_k.$$

Ici $I_1, I_2, \ldots, I_k$ sont certains nombres qui dépendent d'une manière déterminée des coefficients de la forme F, et $I'_1, I'_2, \ldots, I'_k$ dépendent de la même façon des coefficients de F'.

On peut dire alors que $I_1, I_2, \ldots, I_k$ forment un système complet d'*invariants* de la forme F, et, pour que deux formes soient équivalentes, il faut et il suffit qu'elles aient les mêmes invariants.

On peut étendre facilement ces considérations au cas où la forme F dépend de plusieurs séries d'indéterminées, comme cela a lieu pour la forme bilinéaire du n° 22. Et l'on peut aussi considérer simultanément plusieurs formes F, G, ... qui dépendent des mêmes indéterminées.

24. Pour en donner immédiatement un exemple, considérons m fonctions linéaires

$$X_i = a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,m+n}x_{m+n}$$
$$(i = 1, 2, \ldots, m),$$

et un second système analogue

$$X'_i = a'_{i,1}x_1 + a'_{i,2}x_2 + \ldots + a'_{i,m+n}x_{m+n}$$
$$(i = 1, 2, \ldots, m).$$

Comment pourra-t-on reconnaître si les deux systèmes sont équivalents ou non, c'est-à-dire s'il est possible oui ou non de les transformer l'un dans l'autre par une substitution de déterminant ± 1? La réponse est ici immédiate d'après les développements du n° 10. En effet, nous savons que, par une substitution de déterminant ± 1, on peut transformer les X_i dans les Y_i

$$\begin{aligned}
Y_1 &= d_1 y_1,\\
Y_2 &= \beta_{2,1}y_1 + d_2 y_2,\\
Y_3 &= \beta_{3,1}y_1 + \beta_{3,2}y_2 + d_3 y_3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
Y_m &= \beta_{m,1}y_1 + \ldots + \beta_{m,m-1}y_{m-1} + d_m y_m.
\end{aligned}$$

où $d_1, d_2, \ldots, d_m$ sont des nombres positifs, et

$$0 \leqq \beta_{i,k} < d_i \qquad [k = 1, 2, \ldots, (i-1)].$$

Ces nombres d_i, $\beta_{i,k}$ forment maintenant un système complet d'invariants, et, pour que deux systèmes soient équivalents, il faut et il suffit qu'ils admettent les mêmes invariants.

En effet, si les deux systèmes sont équivalents, ils représentent les mêmes systèmes de m nombres, et dès lors leurs invariants sont égaux, car nous avons remarqué (n° 10) que ces invariants dépendent uniquement des divers systèmes de nombres représentés par les formes linéaires. Cette condition de l'égalité des invariants est donc nécessaire pour l'équivalence, mais elle est aussi suffisante manifestement.

On voit que la solution a été obtenue ici en transformant les formes linéaires X_i dans les Y_i qui affectent une forme particulièrement simple. Ce système des Y_i pourrait s'appeler *un système réduit;* il est unique et le même pour tous les systèmes équivalents.

25. Revenons maintenant à la forme bilinéaire

$$F = \sum\sum a_{i,k} x_k y_i$$
$$\left(\begin{matrix} i = 1, 2, \ldots, m \\ k = 1, 2, \ldots, n \end{matrix}\right).$$

En opérant sur les x_k, y_i des substitutions de déterminants ± 1, on obtiendra une forme équivalente

$$F' = \sum\sum a'_{i,k} x_k y_i.$$

Nous allons montrer que, parmi ces formes équivalentes, il y en a toujours une, parfaitement déterminée, qui affecte la forme très simple

$$e_1 x_1 y_1 + e_2 x_2 y_2 + \ldots + e_p x_p y_p,$$

et que nous appellerons la forme *réduite*. Ici $e_1, e_2, \ldots, e_p$ sont des entiers positifs, e_{k-1} divise e_k, et p est tout au plus égal au plus petit des nombres m et n. Ensuite on reconnaîtra facilement que la condition nécessaire et suffisante pour l'équivalence de deux formes bilinéaires consiste en ce qu'elles admettent la même forme réduite. On peut donc considérer les nombres $e_1, e_2, \ldots, e_p$ comme un système complet d'invariants de la forme bilinéaire F.

Considérons la matrice

$$\| a_{i,k} \| \quad \text{ou} \quad \| \mathrm{A} \|.$$

formée par les coefficients de F. Nous désignerons par d_1 le plus grand commun diviseur (pris positivement) des coefficients $a_{i,k}$, par d_2 le plus grand commun diviseur des déterminants du second degré tels que

$$\begin{vmatrix} a_{i,k} & a_{i,l} \\ a_{r,k} & a_{r,l} \end{vmatrix},$$

de même, par d_3 le p. g. c. d. des déterminants du troisième degré, etc.

Si tous les déterminants du degré p ne sont pas nuls, mais si tous les déterminants du degré $p+1$ sont nuls, on aura ainsi la suite des p nombres

$$d_1, \quad d_2, \quad \ldots, \quad d_p,$$

et nous supposerons alors $d_{p+k} = 0$. Il est clair que d_{k-1} divise d_k et nous posons

$$e_1 = d_1, \qquad e_2 = \frac{d_2}{d_1}, \qquad \ldots, \qquad e_p = \frac{d_p}{d_{p-1}}, \qquad e_{p+k} = 0.$$

Ces nombres e sont des entiers, nous les appellerons déjà les *invariants* de F; nous verrons plus loin que e_{k-1} divise e_k; p est tout au plus égal au plus petit des nombres m et n.

Soit maintenant

$$\| a'_{i,k} \| \quad \text{ou} \quad \| A' \|$$

la matrice formée par les coefficients de la forme F' équivalente à la forme F, et d'_k le p. g. c. d. des déterminants de degré k de cette matrice. Il est clair que tout déterminant de degré k de la matrice $\| A' \|$ est une fonction linéaire et homogène de divers déterminants de degré k de la matrice $\| A \|$. Donc d'_k est nécessairement divisible par d_k et tous les déterminants de degré $p+1$ de $\| A' \|$ sont nuls. Mais, pour la même raison, d_k doit être divisible par d'_k; donc

$$d'_k = d_k,$$

et tous les déterminants du degré p de $\| A' \|$ ne peuvent pas être nuls. On voit par là que les deux formes bilinéaires équivalentes F et F' ont les mêmes invariants $e_1, e_2, \ldots, e_p$.

L'égalité des invariants est donc une condition nécessaire pour l'équivalence de deux formes, qu'elle est aussi une condition suffisante; cela résulte ensuite immédiatement de la proposition que nous avons énoncée déjà, d'après laquelle la forme F est équivalente à la forme réduite

$$e_1 x_1 y_1 + e_2 x_2 y_2 + \ldots + e_p x_p y_p.$$

En effet, d'après cela deux formes, dont les invariants sont égaux, sont équiva-

lentes à une même forme réduite, et, par conséquent, aussi équivalentes l'une à l'autre.

26. Nous avons à montrer maintenant comment on peut opérer cette réduction de F à la forme réduite. Considérons la matrice

$$\begin{matrix} a_{1,1}, & a_{1,2}, & a_{1,3}, & \ldots, & a_{1,n}, \\ a_{2,1}, & a_{2,2}, & a_{2,3}, & \ldots, & a_{2,n}, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ a_{m,1}, & a_{m,2}, & a_{m,3}, & \ldots, & a_{m,n}. \end{matrix}$$

Par une substitution sur les x_k, on peut d'abord réduire la première ligne à

$$\delta_1, \quad 0, \quad 0, \quad \ldots, \quad 0,$$

δ_1 étant le p. g. c. d. de $a_{1,1}, a_{1,2}, \ldots, a_{1,n}$. (Il va sans dire que nous n'employons que des substitutions de déterminants $= \pm 1$.)

Si après cela δ_1 divise tous les autres coefficients de la première colonne, on pourra, en remplaçant y_1 par une expression de la forme

$$y_1 + c_2 y_2 + \ldots + c_m y_m,$$

sans changer $y_2, \ldots, y_m$, obtenir une matrice transformée de la forme

$$(\mathrm{A}) \qquad \left\{ \begin{matrix} \delta_1 & 0 & 0 & \ldots & 0 \\ 0 & b_{2,2} & b_{2,3} & \ldots & b_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & b_{m,2} & b_{m,3} & \ldots & b_{m,n}. \end{matrix} \right.$$

Mais si δ_1 ne divisait pas les coefficients de la première colonne, on pourrait diminuer ce coefficient δ_1, et le remplacer par δ_2, le p. g. c. d. des coefficients de la première colonne, en opérant une substitution sur les y, et annuler en même temps les autres coefficients de la première colonne. Si δ_2 divise maintenant tous les coefficients de la première ligne, on obtiendra encore une matrice de la forme (A), en remplaçant x_1 par une expression

$$x_1 + c_2 x_2 + \ldots + c_n x_n,$$

sans changer $x_2, \ldots, x_n$. Au contraire, si δ_2 ne divise pas ces coefficients, on pourra le diminuer encore par une substitution sur les x. Il est clair qu'après un nombre fini d'opérations on obtiendra toujours une forme équivalente, dont la matrice affecte la forme particulière (A); mais on peut simplifier encore et obtenir une matrice (A), dans laquelle δ_1 divise exactement tous les coefficients $b_{i,k}$.

En effet, supposons que δ_1 ne divise pas exactement un des coefficients $b_{i,k}$. Il suffira de remplacer x_k par $x_k + x_1$ pour voir paraître ce coefficient $b_{i,k}$ dans la première colonne avec δ_1. En reprenant alors les opérations de tout à l'heure, on obtiendra un Tableau du type (A), mais dans lequel le coefficient δ_1 a une valeur moindre. On voit donc qu'on peut diminuer ce coefficient tant qu'il ne divise pas tous les $b_{i,k}$, et, après un nombre fini de transformations, on tombera nécessairement sur une forme équivalente à F du type suivant

	x_1	x_2	x_3	$\dots$	x_n
y_1	e_1	0	0	$\dots$	0
y_2	0	$b_{2,2}$	$b_{2,3}$	$\dots$	$b_{2,n}$
y_3	0	$b_{3,2}$	$b_{3,2}$	$\dots$	$b_{3,n}$
..	.	....	....	...	....
y_m	0	$b_{m,2}$	$b_{m,3}$	$\dots$	$b_{m,n}$

et dans laquelle le coefficient e_1 divise tous les autres coefficients $b_{i,k}$.

Et il est clair immédiatement que e_1 est le p. g. c. d. des coefficients $a_{i,k}$. Si maintenant les $b_{i,k}$ ne sont pas tous nuls, on pourra continuer la même réduction en opérant seulement sur les variables $x_2, \dots, x_n, y_2, \dots, y_m$. On obtiendra ainsi une forme équivalente

	x_1	x_2	x_3	$\dots$	x_n
y_1	e_1	0	0	$\dots$	0
y_2	0	e_2	0	$\dots$	0
y_3	0	0	$c_{3,3}$	$\dots$	$c_{3,n}$
..	.	.	...	...	...
y_m	0	0	$c_{m,3}$	$\dots$	$c_{m,n}$

où e_2 est un multiple de e_1 et divise tous les $c_{i,k}$.

En continuant ainsi, on obtiendra finalement la forme réduite

$$e_1 x_1 y_1 + e_2 x_2 y_2 + \dots + e_p x_p y_p.$$

Puisque e_{k-1} divise e_k, il est immédiatement clair que le p. g. c. d. des déterminants de degré k de la matrice correspondante à cette forme réduite est

$$e_1 e_2 \dots e_k = d_k,$$

d'où l'on voit que les e_k ont bien les valeurs indiquées précédemment.

27. Dans la pratique, et s'il s'agit seulement de calculer les invariants, on pourra remplacer souvent avec avantage le procédé que nous venons d'indiquer

par le suivant. Après avoir obtenu une forme équivalente

	x_1	x_2	x_3	$\ldots$	x_n
y_1	δ_1	0	0	$\ldots$	0
y_2	0	$b_{2,2}$	$b_{2,3}$	$\ldots$	$b_{2,n}$
y_3	0	$b_{3,2}$	$b_{3,3}$	$\ldots$	$b_{3,n}$
..	.	...	...	...	....
y_m	0	$b_{m,2}$	$b_{m,3}$	$\ldots$	$b_{m,n}$

dans laquelle δ_1 ne divise pas nécessairement les $b_{i,k}$, on continuera la même transformation sur les indeterminées $x_2, \ldots, x_n, y_2, \ldots, y_m, \ldots$. De cette façon, on finira par obtenir une forme équivalente

$$\delta_1 x_1 y_1 + \delta_2 x_2 y_2 + \ldots + \delta_p x_p y_p,$$

dans laquelle $\delta_1, \delta_2, \ldots, \delta_p$ sont des nombres positifs, et qu'on pourrait appeler une forme *normale*. Il est clair que le p. g. c. d. des déterminants de degré k de la matrice correspondante, qui doit être égal à d_k, est ici simplement le p. g. c. d. des divers produits k à k des nombres

$$\delta_1, \quad \delta_2, \quad \ldots, \quad \delta_p;$$

d'où l'on conclut, d'après les explications du Chap. I (n°s 8-10), que les invariants $e_1, e_2, \ldots, e_p$ sont simplement les nombres *réduits* de $\delta_1, \delta_2, \ldots, \delta_p$. Ayant ainsi obtenu une forme normale, on en conclut donc sans difficulté les invariants. On voit aussi que cette forme normale n'est pas unique comme la forme réduite, mais il existe toujours un nombre fini de formes normales équivalentes à une forme donnée F.

On peut montrer facilement, d'une façon directe, que la forme normale est équivalente à la forme réduite. Considérons pour cela une forme

$$F = \delta_1 x_1 y_1 + \delta_2 x_2 y_2,$$

et posons

$$(\delta_1, \delta_2) = d, \qquad |\delta_1, \delta_2| = m,$$
$$F' = d x'_1 y'_1 + m x'_2 y'_2.$$

On peut maintenant transformer directement F en F' par les substitutions

$$x_1 = \alpha x'_1 + \beta x'_2, \qquad y_1 = \alpha' y'_1 + \beta' y'_2,$$
$$x_2 = \gamma x'_1 + \delta x'_2, \qquad y_2 = \gamma' y'_1 + \delta' y'_2,$$

(1) $$\alpha\delta - \beta\gamma = 1,$$

(2) $$\alpha'\delta' - \beta'\gamma' = 1,$$

En effet, les conditions du problème sont

(3) $$\delta_1\alpha\alpha' + \delta_2\gamma\gamma' = d,$$

(4) $$\delta_1\alpha\beta' + \delta_2\gamma\delta' = 0,$$

(5) $$\delta_1\beta\alpha' + \delta_2\delta\gamma' = 0,$$

(6) $$\delta_1\beta\beta' + \delta_2\delta\delta' = m.$$

Pour y satisfaire, on prendra, pour α', γ', deux nombres premiers entre eux, soumis à cette seule restriction que

$$(\delta_1\alpha', \delta_2\gamma') = (\delta_1, \delta_2) = d.$$

Cela peut se faire évidemment d'une infinité de manières; le plus simple, c'est de prendre $\alpha' = \gamma' = 1$.

On cherchera ensuite deux nombres α et γ qui satisfont à la relation (3), puis on prendra

$$\beta = -\frac{\delta_2\gamma'}{d}, \qquad \delta = +\frac{\delta_1\alpha'}{d},$$

en sorte que la relation (5) se trouve vérifiée et en même temps la relation (1), car

$$\alpha\delta - \beta\gamma = \frac{\delta_1\alpha\alpha' + \delta_2\gamma\gamma'}{d} = 1.$$

Par suite de ces valeurs de β et δ, la relation (6) revient à

$$\frac{\delta_1\delta_2}{d}(\alpha'\delta' - \beta'\gamma') = m,$$

c'est-à-dire elle rentre dans la formule (2), car $\delta_1\delta_2 = md$. Il suffit donc, pour achever la solution, de déterminer β' et δ' par les relations (2) et (4) qui donnent

$$\beta' = -\frac{\delta_2\gamma}{d}, \qquad \delta' = +\frac{\delta_1\alpha}{d}.$$

Il est clair maintenant que, par une application répétée de la transformation que nous venons d'indiquer, on pourra transformer une forme normale

$$\delta_1 x_1 y_1 + \delta_2 x_2 y_2 + \ldots + \delta_p x_p y_p$$

dans la forme réduite

$$e_1 x_1 y_1 + e_2 x_2 y_2 + \ldots + e_p x_p y_p.$$

28. On peut énoncer le résultat principal que nous venons d'obtenir sous une forme un peu différente; mais, pour simplifier, nous supposerons $m = n$ et le déterminant $|a_{i,k}|$ différent de zéro, en sorte que $p = n$.

La forme bilinéaire

$$F=\sum_1^n\sum_1^n a_{i,k}x_k y_i = X_1 y_1 + X_2 y_2 + \ldots + X_n y_n,$$

$$X_i = a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n$$

est réductible à la forme réduite

$$F' = e_1 x'_1 y'_1 + e_2 x'_2 y'_2 + \ldots + e_n x'_n y'_n$$

par les substitutions

$$x_i = \sum_1^n e_{i,k}x'_k, \qquad y_i = \sum_1^n f_{i,k}y'_k.$$

Supposons qu'on ait

$$x'_i = \sum_1^n p_{i,k}x_k, \qquad y'_i = \sum_1^n q_{i,k}y_k.$$

Si l'on substitue ces valeurs des y'_i dans F', le coefficient de y_i est nécessairement égal à X_i : donc

$$X_i = e_1 q_{1,i}x'_1 + e_2 q_{2,i}x'_2 + \ldots + e_n q_{n,i}x'_n$$

ou bien

(I) $$X_i = q_{1,i}t_1 + q_{2,i}t_2 + \ldots + q_{n,i}t_n,$$

si l'on pose

(II) $$t_1 = e_1 x'_1, \qquad t_2 = e_2 x'_2, \qquad \ldots, \qquad t_n = e_n x'_n.$$

On voit donc que toute substitution

$$X_i = a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n$$
$$(i = 1, 2, \ldots, n)$$

peut être remplacée par trois substitutions successives, la première (I), de déterminant ± 1 introduisant les variables $t_1, t_2, \ldots, t_n$, la seconde affectant la forme particulière (II), tandis que la troisième

(III) $$x'_i = \sum_1^n p_{i,k}x_k$$

a encore un déterminant égal à ± 1.

Il est à peine nécessaire de dire que, dans cet énoncé, on pourrait remplacer les invariants $e_1, e_2, \ldots, e_n$ par les coefficients $\delta_1, \delta_2, \ldots, \delta_n$ d'une forme nor-

male équivalente à F. Et le cas $p < n$ n'apporte non plus une modification ; on aura seulement alors $e_k = 0$ ou $\delta_k = 0$ pour $k > p$.

Le nombre p que nous avons vu s'introduire dans l'étude de la forme bilinéaire

$$F = \sum\sum a_{i,k} x_k y_i$$

$$\begin{pmatrix} i = 1, 2, \ldots, m \\ k = 1, 2, \ldots, n \end{pmatrix}$$

s'appelle le *rang* de la forme bilinéaire ou de la matrice des $a_{i,k}$.

Nous dirons quelquefois aussi que $e_1, e_2, \ldots, e_p$ sont les invariants de cette matrice.

29. L'invariant e_k a été défini d'abord par le quotient $d_k : d_{k-1}$; M. Smith a obtenu encore une autre expression remarquable de cet invariant.

Considérons un déterminant quelconque du degré k de la matrice. Divisons ce déterminant par le p. g. c. d. de ses propres mineurs, soit E_k enfin le p. g. c. d. de tous les quotients qu'on obtient ainsi ; alors le théorème de M. Smith consiste en ce qu'on a

$$E_k = e_k.$$

Pour éviter toute ambiguïté, ajoutons que, lorsqu'un des déterminants de degré k est nul, on doit adopter toujours la valeur zéro pour le quotient obtenu en divisant le déterminant par le p. g. c. d. de ses mineurs, même si ces derniers étaient tous nuls.

Il convient du reste, dans ces considérations, de regarder zéro comme le p. g. c. d. de plusieurs nombres qui sont tous nuls. C'est seulement avec cette convention que le principe du n° 6 (Chap. I) reste applicable au cas où l'on n'exclut pas la valeur zéro pour les nombres $a, b, c, \ldots, l$.

Nous allons démontrer d'abord un cas particulier du théorème de M. Smith. Supposons $n \geq m$ dans la matrice

$$\begin{Vmatrix} a_{1,1} & \cdots & a_{1,n} \\ a_{m,1} & \cdots & a_{m,n} \end{Vmatrix} = \| A \|,$$

nous ferons voir que $E_m = e_m = d_m : d_{m-1}$. Nous pouvons supposer que d_m n'est pas nul, car on aurait, dans le cas contraire, $E_m = e_m = 0$, et l'on peut écrire (*voir* n° 9)

$$\| A \| = \| B \| \times \| C \|,$$

$\| B \|$ étant une matrice du type $m \times m$, $\| C \|$ une matrice du même type que $\| A \|$ dont le plus grand diviseur est l'unité. On reconnaît aisément que les matrices $\| A \|$

et $\| B \|$ ont les mêmes invariants, car la forme bilinéaire de $x_1, \ldots, x_n, y_1, \ldots, y_m$, dont la matrice est $\| B \|$ complétée par $n - m$ colonnes de zéros, est équivalente à la forme bilinéaire dont la matrice est $\| A \|$. Nous savons de plus qu'on peut écrire

$$\| B \| = \| u \| \times \begin{Vmatrix} e_1 & 0 & 0 & \ldots & 0 \\ 0 & e_2 & 0 & \ldots & 0 \\ . & . & . & \ldots & 0 \\ 0 & 0 & 0 & \ldots & e_m \end{Vmatrix} \times \| v \|,$$

où $| u | = | v | = \pm 1$, donc

$$\| u \|^{-1} \times \| A \| = \begin{Vmatrix} e_1 & 0 & 0 & \ldots & 0 \\ 0 & e_2 & . & \ldots & 0 \\ . & . & . & \ldots & 0 \\ 0 & 0 & 0 & \ldots & e_m \end{Vmatrix} \times \| D \|,$$

$\| D \| = \| v \| \times \| C \|$ étant une matrice du type $m \times n$ dont le plus grand diviseur est l'unité.

Si l'on considère les divers déterminants du degré $m - 1$ de $\| A \|$ qui renferment $m - 1$ colonnes données de cette matrice, on constate que le p. g. c. d. de ces déterminants ne change pas si l'on multiplie la matrice par $\| u \|^{-1}$. On en conclut que le nombre E_m est le même pour les deux matrices

$$\| A \| \quad \text{et} \quad \| u \|^{-1} \times \| A \|;$$

il suffira donc de prouver l'égalité $E_m = e_m$ dans le cas de la matrice

$$\begin{Vmatrix} e_1 & 0 & 0 & \ldots & 0 \\ 0 & e_2 & 0 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & e_m \end{Vmatrix} \times \| D \|.$$

obtenue en multipliant par $e_1, e_2, \ldots, e_m$ les m lignes de $\| D \|$.

Soient $\| \Theta_1 \|, \| \Theta_2 \|, \ldots$ les diverses matrices du type $m \times m$ contenues dans $\| D \|$; $\Theta_1, \Theta_2, \ldots$ leurs déterminants; Ψ_i le p. g. c. d. des mineurs de $\| \Theta_i \|$ qui ne renferment pas la dernière ligne; en sorte que $\frac{\Theta_i}{\Psi_i}$ est entier. Enfin, désignons par ϖ_i le quotient obtenu en divisant le déterminant de

$$(1) \qquad \begin{Vmatrix} e_1 & 0 & 0 & \ldots & 0 \\ 0 & e_2 & 0 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & e_m \end{Vmatrix} \times \| \Theta_i \|$$

par le p. g. c. d. de ses mineurs; il s'ensuivra

$$E_m = (\varpi_1, \varpi_2, \varpi_3, \ldots).$$

Mais il est clair que le p. g. c. d. des mineurs de (1) est divisible par $e_1 e_2 \ldots e_{m-1} = d_{m-1}$, et, d'autre part, ce p. g. c. d. est un diviseur de $d_{m-1} \times \Psi_i$ (car $d_{m-1} \times \Psi_i$ est le p. g. c. d. des mineurs qui ne renferment pas la dernière ligne). Donc, ϖ_i divise $e_m \Theta_i$ et est divisible par $\frac{e_m \Theta_i}{\Psi_i} = \frac{\varpi_i}{\alpha_i}$. On a donc nécessairement

$$\left(\frac{\varpi_1}{\alpha_1}, \frac{\varpi_2}{\alpha_2}, \ldots\right) = N \times e_m,$$

et, d'autre part, e_m est le p. g. c. d. des nombres $e_m \Theta_i = \varpi_i \beta_i$

$$(\varpi_1 \beta_1, \varpi_2 \beta_2, \ldots) = e_m.$$

Le nombre $E_m = (\varpi_1, \varpi_2, \ldots)$ doit donc être un multiple de $N \times e_m$ et un diviseur de e_m, ce qui exige

$$N = 1, \qquad E_m = e_m. \qquad\qquad \text{C. Q. F. D.}$$

A l'aide de ce cas particulier, il est facile d'arriver au théorème général.

Si, dans une matrice quelconque du type $m \times n$, on se propose de calculer le nombre E_k, on peut commencer par choisir k colonnes verticales, puis diviser chacun des déterminants du degré k de cette matrice partielle du type $m \times k$ $(m \geqq k)$ par le p. g. c. d. de ses propres mineurs. Soit λ_i le p. g. c. d. des quotients ainsi obtenus; alors, d'après ce que nous venons de voir, λ_i est le $k^{\text{ième}}$ invariant de la matrice partielle. Par conséquent, λ_i ne changera pas en effectuant sur $y_1, \ldots, y_m$ une substitution de déterminant ± 1. Mais E_k est évidemment le p. g. c. d. des divers nombres $\lambda_1, \lambda_2, \ldots$ correspondant aux divers groupes de k colonnes; donc E_k ne change pas par cette substitution sur y_1, $y_2, \ldots, y_m$. Par le même raisonnement, on voit que E_k ne change pas en effectuant sur les $x_1, \ldots, x_n$ une substitution de déterminant ± 1. E_k est donc le même pour toutes les formes équivalentes à F et, en considérant la forme réduite ou une forme normale, on constate que $E_k = e_k$.

30. La nouvelle expression des invariants conduit à plusieurs conséquences importantes. Soient

$$e_1, \quad e_2, \quad \ldots, \quad e_p$$

les invariants d'une matrice $\|a_{i,k}\|$ ou $\|A\|$. Supprimons dans $\|A\|$ une colonne ou

une ligne, désignons par $\| A' \|$ la matrice ainsi obtenue, et par

$$e'_1, \quad e'_2, \quad \ldots, \quad e'_q$$

ses invariants. Il est clair que $q \leq p$ et ensuite e'_k est divisible de e_k.

Si, au lieu de supprimer une colonne, on avait multiplié les éléments de cette colonne par un nombre entier N, les invariants de la nouvelle matrice $\| A'' \|$ seraient

$$e''_1, \quad e''_2, \quad \ldots, \quad e''_p.$$

et e''_k est divisible par e_k. Soient en effet P_k le p. g. c. d. des déterminants du degré k de $\| A \|$ qui ne renferment pas la colonne que l'on change, Q_k le p. g. c. d. des déterminants qui renferment cette colonne, on aura

$$d_k = (P_k, Q_k), \qquad d'_k = P_k, \qquad d''_k = (P_k, NQ_k),$$
$$d_{k-1} = (P_{k-1}, Q_{k-1}), \qquad d'_{k-1} = P_{k-1}, \qquad d''_{k-1} = (P_{k-1}, NQ_{k-1}) :$$

donc

$$\frac{d''_k}{d_k} = \frac{(P_k, NQ_k)}{d_k} = \frac{(P_k, NQ_k, NP_k)}{d_k} = \frac{(P_k, Nd_k)}{d_k} = \left(\frac{P_k}{d_k}, N\right);$$

de même

$$\frac{d''_{k-1}}{d_{k-1}} = \left(\frac{P_{k-1}}{d_{k-1}}, N\right).$$

Puisque

$$\frac{P_k}{d_k} : \frac{P_{k-1}}{d_{k-1}} = e'_k : e_k$$

est entier, il en est de même de

$$\frac{d''_k}{d_k} : \frac{d''_{k-1}}{d_{k-1}} = e''_k : e_k. \qquad \text{C. Q. F. D.}$$

Il est facile maintenant d'établir les conditions nécessaires et suffisantes pour qu'une forme bilinéaire

$$G = \sum\sum b_{i,k} x'_k y'_i$$

soit contenue dans une forme

$$F = \sum\sum a_{i,k} x_k y_i.$$

En effet, soient

$$x_i = \sum_1^n c_{i,k} x'_k,$$

$$y_i = \sum_1^n f_{i,k} y'_k$$

les deux substitutions qui transforment F en G. On reconnaît d'abord que le rang

de G ne peut pas surpasser le rang de F, car un déterminant quelconque de la matrice $\| b_{i,k} \|$ est une fonction linéaire et homogène des déterminants de $\| a_{i,k} \|$. Chacune des substitutions qui transforment F en G peut être remplacée par une suite de trois substitutions comme au n° 28. Les substitutions de déterminants ± 1 ne changent pas les invariants, mais une substitution telle que

$$t_i = e_i x'_i$$

a évidemment pour effet de multiplier les invariants par certains nombres entiers. Les invariants de G sont donc divisibles par les invariants correspondants de F. On reconnaît facilement que cette condition, qui est nécessaire, est aussi suffisante.

Théorème XI. — *Pour qu'une forme bilinéaire* G *soit contenue dans la forme* F, *il faut et il suffit que le rang de* G *ne surpasse pas le rang de* F, *et que les invariants de* G *soient divisibles par les invariants correspondants de* F.

Ce résultat comprend aussi le cas de l'équivalence.

31. Considérons maintenant les systèmes de congruences linéaires

$$(1)\qquad \left\{ \begin{array}{l} a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n \equiv u_i \pmod{M} \\ \qquad\qquad (i = 1, 2, \ldots, n). \end{array} \right.$$

Désignons par

$$e_i = \frac{d_i}{d_{i-1}}, \qquad \varepsilon_i = \frac{\delta_i}{\delta_{i-1}} \qquad (i = 1, 2, \ldots, n)$$

les invariants de la matrice du système et ceux de la matrice complétée. Nous supposons que d_n ne soit pas nul.

Posons

$$c_i = (M, e_i), \qquad \gamma_i = (M, \varepsilon_i),$$
$$C = c_1 c_2 \ldots c_n, \qquad \Gamma = \gamma_1 \gamma_2 \ldots \gamma_n,$$

alors on peut énoncer

Théorème XII. — *Pour que le système* (1) *admette des solutions, il faut et il suffit qu'on ait*

$$C = \Gamma.$$

Si cette condition est satisfaite, le nombre des solutions est exactement $= C$.

En effet, d'après le théorème VIII, le système (1) admettra des solutions seulement dans le cas où les plus grands diviseurs des deux matrices

$$\left\| \begin{array}{cccccccc} M & 0 & 0 & \ldots & 0 & a_{1,1} & \ldots & a_{1,n} \\ 0 & M & 0 & \ldots & 0 & a_{2,1} & \ldots & a_{2,n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & M & a_{n,1} & \ldots & a_{n,n} \end{array} \right\|$$

et

$$\left\|\begin{matrix} M & 0 & 0 & \ldots & 0 & a_{1,1} & \ldots & a_{1,n} & u_1 \\ 0 & M & 0 & \ldots & 0 & a_{2,1} & \ldots & a_{2,n} & u_2 \\ . & .. & . & \ldots & . & \ldots & \ldots & \ldots & .. \\ 0 & 0 & 0 & \ldots & M & a_{n,1} & \ldots & a_{n,n} & u_n \end{matrix}\right\|$$

sont égaux.

Mais le premier de ces nombres est évidemment égal à

$$\begin{aligned} &(M^n, M^{n-1}d_1, M^{n-2}d_2, \ldots, M d_{n-1} d_n) \\ &\quad = (M^n, M^{n-1}e_1, M^{n-2}e_1e_2 \ldots M e_1 e_2 \ldots e_{n-1}, e_1 e_2 \ldots e_n) \\ &\quad = (M, e_1)\times(M, e_2)\times\ldots\times(M, e_n) = C, \end{aligned}$$

et le second de ces nombres est pour la même raison $= \Gamma$. La première partie du théorème est ainsi démontrée. Pour obtenir le nombre des solutions dans le cas $C = \Gamma$, il suffit de se rappeler que, par une substitution de déterminant ± 1

$$x_i = \sum_1^n \alpha_{i,k} v_k,$$

et, en remplaçant les équations (1) par des combinaisons convenables, on peut obtenir un système équivalent de la forme

$$e_i v_i \equiv f_i \pmod{M}.$$

Or le nombre des solutions de ce dernier système est évidemment

$$(M, e_1)\times(M, e_2)\times\ldots\times(M, e_n) = C.$$

Il est à remarquer que $\gamma_i = (M, \varepsilon_i)$ divise $c_i = (M, e_i)$, car ε_i divise e_i. La condition $C = \Gamma$ exige donc qu'on ait

$$c_i = \gamma_i \qquad (i = 1, 2, \ldots, n).$$

32. On peut donner au théorème XII une autre forme en supposant décomposé en facteurs premiers le module M.

Soient μ, a_k, α_k les exposants des plus hautes puissances d'un nombre premier p, qui divisent respectivement M, d_k, δ_k. Alors on a

$$(1) \qquad a_n - a_{n-1} \geqq a_{n-1} - a_{n-2} \geqq \ldots \geqq a_1 - a_0,$$

$$(2) \qquad \alpha_n - \alpha_{n-1} \geqq \alpha_{n-1} - \alpha_{n-2} \geqq \ldots \geqq \alpha_1 - \alpha_0,$$

$$(3) \qquad a_k \geqq \alpha_k,$$

$$(4) \qquad a_k - a_{k-1} \geqq \alpha_k - \alpha_{k-1}.$$

car nous savons que les rapports

$$e_{k+1} : e_k, \quad \varepsilon_{k+1} : \varepsilon_k, \quad d_k : \delta_k, \quad e_k : \varepsilon_k$$

sont des entiers.

La condition

$$(d_n, d_{n-1}M, d_{n-2}M^2, \ldots, M^n) = (\delta_n, \delta_{n-1}M, \delta_{n-2}M^2, \ldots, M^n)$$

devient maintenant pour chaque nombre premier p qui divise M

$$(5) \qquad (p^{a_n}, p^{a_{n-1}+\mu}, p^{a_{n-2}+2\mu}, \ldots, p^{n\mu}) = (p^{\alpha_n}, p^{\alpha_{n-1}+\mu}, p^{\alpha_{n-2}+2\mu}, \ldots, p^{n\mu}).$$

Supposons que, dans la série (2), le premier terme plus petit que μ soit $\alpha_\sigma - \alpha_{\sigma-1}$; alors la relation (5), qui exprime la condition nécessaire et suffisante pour que les congruences admettent une solution pour le module p^μ, devient

$$\alpha_\sigma = a_\sigma,$$

et le nombre des solutions est alors $p^{\alpha_\sigma+(n-\sigma)\mu}$. C'est ce que l'on trouvera par une discussion facile en s'aidant des inégalités (1), (2), (3), (4).

D'après cela, si l'on avait $\mu > \alpha_n - \alpha_{n-1}$, la condition devient $\alpha_n = a_n$ et le nombre des solutions est p^{α_n}. Ainsi, dans ce cas, il suffirait de calculer d_n et δ_n.

On voit facilement que si, dans la série

$$a_n - \alpha_n \geqq a_{n-1} - \alpha_{n-1} \geqq \ldots \geqq a_1 - \alpha_1 \geqq 0,$$

$a_k - \alpha_k$ est le premier terme égal à zéro, $p^{\alpha_{k+1}-\alpha_k}$, est la plus haute puissance de p pour laquelle, comme module, le système des congruences admet des solutions.

C'est seulement pour préciser les idées que nous avons supposé au n° 31 que le déterminant d_n du système (1) n'était pas nul.

Et aussi, à proprement parler, ce n'est pas là une restriction, car, en ajoutant des multiples de M aux coefficients, on peut toujours faire en sorte qu'il en soit ainsi.

Mais la plus légère attention suffit pour reconnaître que le théorème XII est général et reste vrai même dans le cas où l'on aurait $d_{p+1} = 0$, à condition seulement de se conformer à notre convention de prendre dans ce cas

$$e_{p+1} = e_{p+2} = \ldots = e_n = 0,$$

et de même pour les invariants de la matrice complétée.

33. Considérons maintenant le système

$$a_{i,1}x_1 + \ldots + a_{i,m+n}x_{m+n} \equiv u_i \pmod{M}$$
$$(i = 1, 2, \ldots, n).$$

Désignons comme au n° 31 par

$$e_i = \frac{d_i}{d_{i-1}}, \qquad \varepsilon_i = \frac{\delta_i}{\delta_{i-1}}$$

les invariants de la matrice et de la matrice complétée, puis posons

$$c_i = (\mathrm{M}, e_i), \qquad \gamma_i = (\mathrm{M}, \varepsilon_i),$$
$$\mathrm{C} = c_1 c_2 \ldots c_n,$$
$$\Gamma = \gamma_1 \gamma_2 \ldots \gamma_n.$$

La condition nécessaire et suffisante pour qu'il y ait des solutions est alors encore

$$\mathrm{C} = \Gamma,$$

mais le nombre des solutions est $\mathrm{C} \times \mathrm{M}^m$. En effet, on obtient un système équivalent

$$e_i v_i \equiv f_i \qquad (\bmod \mathrm{M}),$$
$$i = 1, 2, \ldots, n$$

et $v_{n+1}, v_{n+2}, \ldots, v_{n+m}$ restent arbitraires.

34. Soit enfin le système

$$a_{i,1} x_1 + \ldots + a_{i,n} x_n \equiv u_i \qquad (\bmod \mathrm{M}),$$
$$(i = 1, 2, \ldots, n+m),$$

et désignons toujours par

$$e_i = \frac{d_i}{d_{i-1}} \qquad (i = 1, 2, \ldots, n),$$
$$\varepsilon_i = \frac{\delta_i}{\delta_{i-1}} \qquad (i = 1, 2, \ldots, n+1)$$

les invariants de la matrice et de la matrice complétée.

La condition nécessaire et suffisante pour qu'il y ait des solutions s'obtient à l'aide du théorème VIII sous la forme

$$(\alpha) \qquad \left\{ \begin{aligned} & (\mathrm{M}^{n+m}, \mathrm{M}^{n+m-1} d_1, \mathrm{M}^{n+m-2} d_2, \ldots, \mathrm{M}^m d_n) \\ & = (\mathrm{M}^{n+m}, \mathrm{M}^{n+m-1} \delta_1, \mathrm{M}^{n+m-2} \delta_2, \ldots, \mathrm{M}^{m-1} \delta_{n+1}) \end{aligned} \right.$$

ou, après une réduction facile,

$$(\alpha') \qquad \left\{ \begin{aligned} & \mathrm{M} \times (\mathrm{M}, e_1) \times (\mathrm{M}, e_2) \times \ldots \times (\mathrm{M}, e_n) \\ & \quad = (\mathrm{M}, \varepsilon_1) \times (\mathrm{M}, \varepsilon_2) \times \ldots \times (\mathrm{M}, \varepsilon_{n+1}). \end{aligned} \right.$$

Mais, puisque (M, ε_k) divise (M, e_k), on a nécessairement

(1) $$\varepsilon_{n+1} \equiv 0 \pmod{M}.$$

Par conséquent $M^m \delta_n$ divise $M^{m-1}\delta_{n+1}$, et au lieu de (α) on peut écrire

$$\begin{aligned} &(M^{n+m}, M^{n+m-1}d_1, \ldots, M^m d_n) \\ &= (M^{n+m}, M^{n+m-1}\delta_1, \ldots, M^m \delta_n), \end{aligned}$$

ce qui revient encore à

(2) $$C = \Gamma,$$

si l'on pose comme précédemment

$$C = (M, e_1) \times (M, e_2) \times \ldots \times (M, e_n),$$
$$\Gamma = (M, \varepsilon_1) \times (M, \varepsilon_2) \times \ldots \times (M, \varepsilon_n).$$

Pour qu'il y ait des solutions, les conditions (1) et (2) sont nécessaires et suffisantes. Le nombre des conditions s'obtient sans difficulté ; il est égal à C.

35. Les méthodes développées à partir du nº 22 permettent de retrouver avec facilité la plupart des résultats obtenus dans la première Partie de ce Chapitre. Nous nous bornerons à déduire de cette façon le théorème VIII sous une forme plus générale. Considérons donc les équations non homogènes

(I) $$\begin{cases} a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n + a_{i,n+1} = 0 \\ \qquad (i = 1, 2, \ldots, m) \end{cases}$$

sans faire aucune hypothèse sur m et n. Soient $\|A\|$ et $\|A'\|$ la matrice du système et la matrice complétée. Si l'on prend k des m équations et que l'on considère tous les déterminants du degré k qu'on peut former avec leurs coefficients, ces déterminants appartiennent en partie à la matrice $\|A'\|$. Mais, si le système (I) admet une solution, on pourra remplacer les $a_{i,n+1}$ par leurs valeurs

$$-(a_{i,1}x_1 + a_{i,2}x_2 + \ldots + a_{i,n}x_n),$$

en sorte que chaque déterminant de $\|A'\|$ s'exprime en fonction linéaire homogène des déterminants de $\|A\|$. Dans tous les k équations, le p. g. c. d. des déterminants de $\|A\|$ est donc égal au p. g. c. d. des déterminants de $\|A'\|$. D'où l'on conclut que le p. g. c. d. de *tous* les déterminants du degré k est le même pour les deux matrices $\|A\|$ et $\|A'\|$. Ce sont là des conditions *nécessaires* pour

que le système (I) admette des solutions. Mais ces conditions ne sont pas toutes indépendantes, comme cela résulte du théorème suivant :

Théorème XIII. — *Pour que le système* (I) *admette une ou plusieurs solutions, il faut et il suffit que le rang p de $\| A \|$ soit égal au rang de $\| A' \|$, et que le p. g. c. d. des déterminants du degré p soit le même pour les matrices $\| A \|$ et $\| A' \|$.*

Nous avons à démontrer seulement que ces conditions sont suffisantes. Or, par une substitution

$$x_i = \sum_1^n a_{i,k} v_k,$$

et en remplaçant les équations (I) par des combinaisons convenables, on peut obtenir un système absolument équivalent

$$\text{(II)} \quad \begin{cases} e_1 v_1 + u_1 = 0, \quad e_2 v_2 + u_2 = 0, \quad \ldots, \quad e_p v_p + u_p = 0, \\ u_{p+1} = 0, \quad u_{p+2} = 0, \quad \ldots, \quad u_m = 0. \end{cases}$$

Dans cette transformation les rangs de $\| A \|$ et de $\| A' \|$ se conservent, de même que les p. g. c. d. des déterminants du degré k. Puisqu'on suppose que le rang de $\| A' \|$ est $= p$, les déterminants du degré $p + 1$

$$e_1 e_2 \ldots e_p u_{p+1}, \quad e_1 e_2 \ldots e_p u_{p+2}, \quad \ldots, \quad e_1 e_2 \ldots e_p u_m$$

doivent s'annuler ; donc

$$u_{p+1} = u_{p+2} = \ldots = u_m = 0,$$

ce qui montre que les équations (II) ne sont pas incompatibles. De plus, les déterminants du degré p de la matrice $\| A' \|$ transformée

$$e_1 e_2 \ldots e_p, \quad u_1 e_2 e_3 \ldots e_p, \quad e_1 u_2 e_3 \ldots e_p, \quad \ldots, \quad e_1 e_2 \ldots e_{p-1} u_p$$

doivent être divisibles par $e_1 e_2 \ldots e_p$. Donc $u_1, u_2, \ldots, u_p$ sont divisibles par $e_1, e_2, \ldots, e_p$ respectivement, en sorte que les équations (II) sont satisfaites par des valeurs *entières* de $v_1, v_2, \ldots, v_p$. C. Q. F. D.

La plupart des résultats de ce Chapitre sont dus à M. Smith ; un seul, le théorème VIII avait été obtenu antérieurement par M. I. Heger. Le même sujet a été repris ensuite par M. Frobenius qui a introduit la forme bilinéaire. Le Mémoire de M. Frobenius contient encore d'autres applications intéressantes à la théorie *algébrique* des formes bilinéaires.

BIBLIOGRAPHIE.

I. Heger, *Mémoires de l'Académie de Vienne*, t. XIV.

H. J. S. Smith, *On systems of linear indeterminate equations and congruences* (*Philosophical Transactions*, vol. 151; 1861).

H. J. S. Smith, *Arithmetical Notes.*

I. On the arithmetical invariants of a rectangular matrix, of which the constituents are integral numbers.

II. On systems of linear congruences.

III. On an arithmetical demonstration of a theorem in the integral Calculus (*Proceedings of the London mathematical Society*, vol. IV, 1873).

G. Frobenius, *Theorie der linearen Formen mit ganzen Coefficienten* (*Journal de Borchardt*, t. 86; 1879, et t. 88; 1880.)

Ch. Méray, *Solution du problème général de l'Analyse indéterminée du premier degré* (*Annales scientifiques de l'École Normale supérieure*, 2[e] série, t. XII; 1883).

L. Kronecker, *Reduction der Systeme von n^2 ganzzahligen Elementen* (*Journal de Kronecker*, t. CVII; 1890).

ERRATA.

Pages	Lignes.		
36,	7,	en remontant,	*lisez :* $f(x) = (x-\alpha)^a(x-\beta)^b\ldots(x-\lambda)^l f_1(x) \pmod p$.
47,	2,	en remontant,	*au lieu de* Smyth, *lisez :* Smith.
48,	6,	en descendant,	*au lieu de* Smyth, *lisez :* Smith.
72,	7,	en descendant,	*au lieu de* Smyth, *lisez :* Smith.

TABLE DES MATIÈRES.

17255 PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET FILS, QUAI DES GRANDS-AUGUSTINS, 55.

17255 Paris. — Imprimerie GAUTHIER-VILLARS ET FILS, quai des Grands-Augustins, 55.